IBM Tivoli Remote Control

Benutzerhandbuch

Version 3.8

SC12-3220-00

IBM Tivoli Remote Control

Benutzerhandbuch

Version 3.8

SC12-3220-00

Hinweis

Bevor Sie diese Informationen und das dadurch unterstützte Produkt verwenden, lesen Sie die Informationen unter „Bemerkungen" auf Seite 163.

- Die IBM Homepage finden Sie im Internet unter: **ibm.com**
- IBM und das IBM Logo sind eingetragene Marken der International Business Machines Corporation.
- Das e-business-Symbol ist eine Marke der International Business Machines Corporation.
- Infoprint ist eine eingetragene Marke der IBM.
- ActionMedia, LANDesk, MMX, Pentium und ProShare sind Marken der Intel Corporation in den USA und/oder anderen Ländern.
- C-bus ist eine Marke der Corollary, Inc. in den USA und/oder anderen Ländern.
- Java und alle auf Java basierenden Marken und Logos sind Marken der Sun Microsystems, Inc. in den USA und/oder anderen Ländern.
- Microsoft Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.
- PC Direct ist eine Marke der Ziff Communications Company in den USA und/oder anderen Ländern.
- SET und das SET-Logo sind Marken der SET Secure Electronic Transaction LLC.
- UNIX ist eine eingetragene Marke der Open Group in den USA und/oder anderen Ländern.
- Marken anderer Unternehmen/Hersteller werden anerkannt.

Erste Ausgabe (Januar 2003)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Tivoli Remote Control User's Guide, Version 3.8,
IBM Form SC23-4842-00,
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 1996, 2003
© Copyright IBM Deutschland GmbH 2003

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
Januar 2003

Inhaltsverzeichnis

Vorwort vii
Zielgruppe vii
Inhalt dieses Handbuchs vii
Veröffentlichungen ix
Bibliothek von Tivoli Remote Control ix
Vorausgesetzte Literatur ix
Referenzliteratur ix
Online-Veröffentlichungen ix
Veröffentlichungen bestellen x
Rückmeldungen zu Veröffentlichungen x
Eingabehilfen x
Kundenunterstützung anfordern xi
In diesem Handbuch verwendete Konventionen . . xi
Schriftbildkonventionen xi
Betriebssystemabhängige Variablen und Pfade . . xi
Symbol für Tivoli Remote Control xii

Kapitel 1. Übersicht zu Tivoli Remote Control 1
Funktionen in Tivoli Remote Control 1
Komponenten von Tivoli Remote Control 1
Steuerung der Tivoli Remote Control-Sicherheit . . . 2
Berechtigungsklassen 2
Standardrichtlinie 3
Generierung von Hinweisen 3
Generierung von Protokollen und Traces 3
Datenverschlüsselung 4
Aktivierung der Firewall 4
Neue Funktionen in Tivoli Remote Control Version 3.8 4

Kapitel 2. Planung und Installation von Tivoli Remote Control 5
Einführung 5
Voraussetzungen 6
Hardwarevoraussetzungen 6
Unterstützte Hardwareplattformen 6
Voraussetzungen bezüglich des Arbeitsspeichers 7
Voraussetzungen bezüglich des Festplattenspeichers 7
Softwarevoraussetzungen 8
Erforderliche Benutzerberechtigungen auf Windows-Endpunkten 8
Schritt 1: Tivoli Remote Control installieren und Sitzung starten. 8
Schritt 2: Eine Sitzung ausführen 9
Tivoli Remote Control installieren 9
Komponenten, unterstützte Betriebssysteme und Protokolle 10
Schritt 1: Tivoli Remote Control-Server auf verwalteten Knoten installieren 12
Tivoli Software Installation Service (SIS) verwenden. 12
Über den Tivoli-Desktop 12
Den Befehl 'winstall' verwenden 13
Schritt 2: Controller und Ziele auf Endpunkten installieren. 14
Den Treiber von IBM Tivoli Remote Control auf Windows XP-Zielrechnern installieren . . 15
Sitzung im eingeschränkten Modus 16
Integration mit der Datenbank für Tivoli Inventory 16
Schritt 3: Das Tivoli Remote Control-Gateway auf verwalteten Knoten installieren 16
Schritt 4: Den Tivoli Remote Control-Proxy installieren 17
Upgrades von früheren Releases 17
Upgrade einer einzelnen Tivoli Management Region (TMR) 17
Ein Upgrade für einen Bereich von Version 3.7.1 auf Version 3.8 ausführen 17
Upgrade-Methoden. 20
Upgrade für verbundene Bereiche ausführen . . 22
Unterschiedliche Versionen in verbundenen Bereichen verwenden 22
Tivoli Remote Control deinstallieren 22
Den Controller oder das Ziel deinstallieren . . . 22
Den Tivoli Remote Control-Server deinstallieren 22
Den Tivoli Remote Control-Proxy deinstallieren 23

Kapitel 3. Sitzungen über Firewalls ausführen 25
Einführung 25
Identifikation Ihrer Szenarios 25
Szenarios, die auf Firewall Security Toolbox basieren 26
Controller auf der geschützten Seite 27
Controller auf der ungeschützten Seite . . . 28
Controller und Ziel außerhalb von Firewalls 29
Verwendung von mehreren Relays. 30
Szenario mit dem Remote Control-Proxy im Standalone-Modus 31
Ziel und Controller, die zu verbundenen Bereichen gehören, sind durch eine Firewall voneinander getrennt 31
Den Remote Control-Proxy als übergeordnetes oder untergeordnetes Element definieren 31
Mit Tivoli Firewall Security Toolbox arbeiten . . 32
Mit Remote Control-Proxys im Standalone-Modus arbeiten 33
Richtlinienmethode 'rc_def_proxy' für den Zielproxy konfigurieren 33
Den Tivoli Remote Control-Proxy installieren . . . 33
Grafische Benutzerschnittstelle verwenden . . . 33
Übergeordneter Remote Control-Proxy zusätzlich zum Endpunktproxy 34
Untergeordneter Remote Control-Proxy zusätzlich zum Gateway-Proxy 37

Übergeordneter Remote Control-Proxy im Standalone-Modus 40
Untergeordneter Remote Control-Proxy im Standalone-Modus 45
Antwortdatei verwenden 49
Das Relay installieren 50
Den Remote Control-Proxy konfigurieren 51
Log (übergeordneter und untergeordneter Remote Control-Proxy) 51
Communication-layer (übergeordneter Remote Control-Proxy) 51
Communication-layer (untergeordneter Remote Control-Proxy) 53
Children-cm-info (Übergeordneter Remote Control-Proxy) 54
Parent-cm-info (Untergeordneter Remote Control-Proxy) 55
Rcproxy (Übergeordneter und untergeordneter Remote Control-Proxy) 56
Den Pfad für untergeordnete Proxys in Szenarios mit dem Remote Control-Proxy im Standalone-Modus definieren 58
Ein Beispielszenario 59
Unternehmensweite Architektur 59
Firewall-Konnektivität 60
Gateway-Proxy fireA1 61
Endpunktproxy fireA2 61
Zielproxy rcA1 62
Controller-Proxy rcA2 62
Endpunktproxy fireB1 63
Gateway-Proxy fireB2 63
Zielproxy rcB1 64
Controller-Proxy rcB2 64

Kapitel 4. Die Tivoli-Umgebung für die Verwendung der Tivoli Remote Control-Schnittstellen konfigurieren 65
Fernverbindungen aktivieren 65
Einen speziellen Tivoli-Administrator für die Webschnittstelle definieren 65

Kapitel 5. Richtlinienbereiche für die Verwendung von Tivoli Remote Control konfigurieren 67
Schritt 1: Die verwaltete Remote Control-Ressource zu einem Richtlinienbereich hinzufügen 67
Schritt 2: Ein Remote Control-Tool im Richtlinienbereich erstellen 67
Schritt 3: Tivoli Remote Control-Berechtigungsklassen zuordnen 69
Schritt 4: Richtlinienbereichen Ziele zuordnen . . . 70

Kapitel 6. Standardeinstellungen des Remote Control-Tools ändern 71
Remote Control-Standardrichtlinie ändern 71
Schritt 1: Kopie der Remote Control-Standardrichtlinie erstellen 71
Schritt 2: Inhalt einer Richtlinienmethode anpassen 72
Schritt 3: Neue Remote Control-Standardrichtlinie zuordnen 73
Über den Tivoli-Desktop 73
Über die Befehlszeile 73
Zusammenfassung der Standardrichtlinienmethoden 73
Tivoli Remote Control-Richtlinienmethoden . . . 74
rc_def_alt_t 75
rc_def_backgrnd 75
rc_def_color 75
rc_def_command 76
rc_def_comp 76
rc_def_define 77
rc_def_encryption 77
rc_def_ftmode 78
rc_def_grace_time 78
rc_def_gw 79
rc_def_inactivity 79
rc_def_initstate 80
rc_def_optimize 80
rc_def_polfilter_mode 80
rc_def_ports 81
rc_def_proxy 82
rc_def_rate 83
rc_def_rcmode 83
rc_def_targets. 84
rc_def_timeout_op 84
rc_def_uncheckedlist 84

Kapitel 7. Tivoli Remote Control-Schnittstelle anpassen 87
Zielmaschinenliste anpassen 87
Für 'rc_def_define' den Wert 'DefinableTargetList' festlegen 88
Für 'rc_def_define' den Wert 'FilteredList' festlegen 88
Für 'rc_def_define' den Wert 'UncheckedList' festlegen 89
Vorhandene Zielmaschinenliste über einen Dialog ändern 89
Sitzungseinstellungen anpassen. 90
Tivoli Remote Control-Webseite anpassen 91

Kapitel 8. Tivoli Remote Control starten 93
Eine Tivoli Remote Control-Aktion starten 93
Über den Tivoli-Desktop starten 93
Dialog mit Zielmaschinenliste 93
Dialog mit Richtlinienbereichs- und Zielmaschinenliste 94
Über einen Web-Browser starten 95
Über eine Terminal Server-Umgebung starten . . 97
Über die Befehlszeile starten. 98
Tivoli Remote Control-Gateway starten 99
Tivoli Remote Control-Proxy starten 99

Kapitel 9. Aktionen 'Remote Control' und 'Neustart' verwenden 101
Aktion 'Remote Control' verwenden. 101
Remote Control-Sitzungen starten und beenden 101
Das Fenster 'Remote Control' 102

Sitzungsstatus ändern 102
Status vom Controller aus ändern 102
Status vom Zielrechner aus ändern 103
In andere Tastaturmodi umschalten 104
Systemtastenkombinationen senden 104
Einschränkungen bei der Tastatureingabe auf einem OS/2-Gateway 105
Verschiedene Tastaturen verwenden 105
Tastaturen synchronisieren 106
Aktion 'Neustart' verwenden 106

Kapitel 10. Aktion 'Chat' verwenden 107
Chat-Sitzungen starten und beenden 107
Das Fenster 'Chat' 107
Nachrichten austauschen 109
Chat-Sitzungen suspendieren und erneut aktivieren 109
Chat-Dialoge protokollieren 110
Chat-Ereignisse protokollieren 110
Chat bei Remote Control-Sitzungen verwenden . . 111

Kapitel 11. Aktion 'Dateiübertragung' verwenden 113
Dateiübertragungssitzungen starten und beenden 113
Das Fenster 'Dateiübertragung' 114
Dateien kopieren 115
Verzeichnisse erstellen 115
Verzeichnisse und Dateien löschen 115
Dateiübertragungsereignisse protokollieren . . . 116

Kapitel 12. Fehlerbehebung und Leistungsoptimierung 117
Fehlerbehebung 117
Tivoli Remote Control-Protokolle festlegen. . . 117
Remote Control-Ereignisse auf dem Controller und auf dem Zielrechner protokollieren . 117
Dateiübertragungsereignisse auf dem Controller und auf dem Zielrechner protokollieren 118
Chat-Ereignisse auf dem Controller und auf dem Zielrechner protokollieren 119
Inhalt der Protokolldateien 120
Installationsinformationen auf dem Remote Control-Server protokollieren 121
Tivoli Remote Control-Traces festlegen 121
Traces auf dem Remote Control-Server festlegen 121
Traces auf einem Windows-Controller und -Zielrechner festlegen 122
Traces auf einem OS/2-Controller und -Zielrechner festlegen 127
Inhalt der Tracedatei 127
Zusammenfassung der Tivoli Remote Control-Protokolle und -Traces 128
Anwendungsereignisse auf einem Windows NT-, Windows 2000- oder Windows XP-Controller protokollieren 130
Tivoli Enterprise Console verwenden . . . 131
Tivoli-Server-Traces festlegen 132
Endpunktfehler protokollieren 132
Umgebungsinformationen sammeln 132
Workstation-Konfigurationsbericht 133
Tastaturbelegungsprotokoll 133
Leistung steigern 133
Zielrechner schnell in die Zielmaschinenliste laden 135

Anhang A. Eingabehilfen 137
In der Schnittstelle mit Hilfe der Tastatur navigieren 137
Vergrößerung der Bildschirmanzeige 137

Anhang B. Häufig gestellte Fragen 139
Installation 139
Steuern und Überwachen 140
Befehlszeile 142
Deinstallation 142
Fehlernachrichten 143

Anhang C. Bei der Installation geänderte Registrierungsdatenbanken und Dateien 145
Windows Controller-Registrierungsdatenbank . . 145
Datei von OS/2-Controllern 145
CONFIG.SYS 145
Dateien von Windows 98 Second Edition-Zielrechnern 145
SYSTEM.INI 145
Registrierungsdatenbank von Windows 98 Second Edition-Zielrechnern 145
Registrierungsdatenbank von Windows NT-, Windows 2000- und Windows XP-Zielrechnern . . . 146
Dateien von OS/2-Zielrechnern 147
CONFIG.SYS 147
SYSTEM.INI 147
OS2.INI 147

Anhang D. Befehlszeilenschnittstelle 149
Befehlszeilensyntax 149
rcproxy 150
wcreatecontroller 151
wcreaterc 152
wdeletecontroller 153
wrc 154
wrcinstep 157
wrcmdpcr 159
wrcuninstep 161

Bemerkungen 163
Marken 164

Glossar 165

Index 169

Vorwort

Tivoli® Remote Control ermöglicht einem Systemadministrator, mit Hilfe eines ***Controllers*** (Workstation des Administrators) verschiedene Arbeitsgänge auf einem ***Ziel*** (ferne Workstation) auszuführen. Controller und Ziele müssen Endpunkte sein.

In Tivoli Remote Control können folgende Aktionen ausgeführt werden:

Fernsteuerung	Ermöglicht dem Administrator die Steuerung von Tastatur- und Mauseingaben sowie die Überwachung der Anzeigeausgabe auf Zielen.
Neustart	Ermöglicht dem Administrator den Neustart von Zielen.
Dateiübertragung	Ermöglicht dem Administrator, Dateien oder Verzeichnisse an Ziele zu senden bzw. von dort zu empfangen.
Chat	Ermöglicht dem Administrator, schriftlich mit dem Benutzer eines Ziels zu kommunizieren.

HINWEIS: Aufgrund von Terminologieänderungen und Änderungen in der Schreibweise bestimmter Begriffe kann es zu Abweichungen zwischen Abbildungen und Text kommen. Unter Umständen sind in diesem Handbuch englische Abbildungen enthalten.

Zielgruppe

Dieses Handbuch richtet sich an Systemadministratoren, die Tivoli Remote Control zur Verwaltung verteilter Systeme einsetzen. Benutzer dieses Handbuchs sollten zumindest mit der aktiven Verwendung von Tivoli Management Framework vertraut sein.

Inhalt dieses Handbuchs

Dieses Handbuch enthält folgende Abschnitte:

- Kapitel 1, „Übersicht zu Tivoli Remote Control", auf Seite 1

  Dieses Kapitel enthält eine Einführung in Tivoli Remote Control und eine Beschreibung der Funktionen, plattformspezifischen Optionen, Terminologie und Sicherheit in Tivoli Remote Control.
- Kapitel 2, „Planung und Installation von Tivoli Remote Control", auf Seite 5

  Dieses Kapitel enthält Hinweise zur Planung und Installation der entsprechenden Komponenten von Tivoli Remote Control.
- Kapitel 3, „Sitzungen über Firewalls ausführen", auf Seite 25

  Dieses Kapitel enthält Informationen, wie der Tivoli Remote Control-Proxy installiert und konfiguriert werden muss, damit Tivoli Remote Control auch bei Einsatz von Firewalls ordnungsgemäß funktioniert.
- Kapitel 4, „Die Tivoli-Umgebung für die Verwendung der Tivoli Remote Control-Schnittstellen konfigurieren", auf Seite 65

  In diesem Kapitel wird beschrieben, wie die Tivoli-Umgebung für die Verwendung der Tivoli Remote Control-Schnittstellen konfiguriert werden muss.

- Kapitel 5, „Richtlinienbereiche für die Verwendung von Tivoli Remote Control konfigurieren", auf Seite 67

  In diesem Kapitel wird erläutert, wie Richtlinienbereiche für die Verwendung von Tivoli Remote Control konfiguriert werden.
- Kapitel 6, „Standardeinstellungen des Remote Control-Tools ändern", auf Seite 71

  In diesem Kapitel wird beschrieben, wie die Einstellungen für das Remote Control-Tool über die Richtlinienmethoden geändert werden.
- Kapitel 7, „Tivoli Remote Control-Schnittstelle anpassen", auf Seite 87

  In diesem Kapitel wird erläutert, wie die Tivoli Remote Control-Schnittstelle über die Schnittstelle oder durch Ändern der Standardrichtlinie, die der Remote-Control-verwalteten Ressource eines Richtlinienbereichs zugeordnet ist, angepasst wird.
- Kapitel 8, „Tivoli Remote Control starten", auf Seite 93

  In diesem Kapitel wird beschrieben, wie eine Sitzung in Tivoli Remote Control gestartet wird.
- Kapitel 9, „Aktionen 'Remote Control' und 'Neustart' verwenden", auf Seite 101

  In diesem Kapitel wird die Verwendung der Aktion 'remote control' (Fernsteuerungsaktion) zum Überwachen oder Steuern einer Zielmaschine beschrieben. Außerdem wird erläutert, wie Sie eine Zielmaschine mit Hilfe der Aktion 'Neustart' neu starten können.
- Kapitel 10, „Aktion 'Chat' verwenden", auf Seite 107

  In diesem Kapitel wird die Verwendung der Aktion 'Chat' zum Austauschen von Nachrichten mit dem Zielmaschinenbenutzer beschrieben.
- Kapitel 11, „Aktion 'Dateiübertragung' verwenden", auf Seite 113

  In diesem Kapitel wird die Verwendung der Aktion 'Dateiübertragung' zum Übertragen von Dateien bzw. Verzeichnissen zwischen Controller und Zielmaschine beschrieben.
- Kapitel 12, „Fehlerbehebung und Leistungsoptimierung", auf Seite 117

  Dieses Kapitel enthält eine Übersicht zu den Tasks, die Sie ausführen müssen, um Informationen zur Fehlerbehebung in Tivoli Remote Control zu erfassen. Außerdem werden in diesem Kapitel die erfassten Informationen beschrieben.

  Im zweiten Teil dieses Anhangs wird beschrieben, wie Sie die Leistung von Tivoli Remote Control optimieren können.
- Anhang A, „Eingabehilfen", auf Seite 137

  In diesem Anhang werden die Funktionen beschrieben, die Personen mit Behinderungen bei der Verwendung von Tivoli Remote Control unterstützen.
- Anhang B, „Häufig gestellte Fragen", auf Seite 139

  Dieser Anhang enthält eine Liste mit häufig gestellten Fragen zu Tivoli Remote Control.
- Anhang C, „Bei der Installation geänderte Registrierungsdatenbanken und Dateien", auf Seite 145

  In diesem Anhang werden die Änderungen an den Konfigurationsdateien von Maschinen mit Windows® 98 Second Edition und OS/2® sowie der Registrierungsdatenbank von Maschinen mit Windows NT®, Windows 2000, Windows XP und Windows 98 Second Edition beschrieben.
- Anhang D, „Befehlszeilenschnittstelle", auf Seite 149

  Dieser Anhang enthält Informationen zu den Tivoli Remote Control-Befehlen, die Sie auf den Workstations ausführen können, auf denen der Remote Control-Server installiert ist.

Veröffentlichungen

In diesem Abschnitt werden Veröffentlichungen in der Bibliothek von *Tivoli Remote Control* sowie andere zugehörige Dokumente aufgelistet. Außerdem wird beschrieben, wie Sie online auf Tivoli-Veröffentlichungen zugreifen, Tivoli-Veröffentlichungen bestellen und Kommentare zu Tivoli-Veröffentlichungen abgeben können.

Bibliothek von Tivoli Remote Control

Die folgenden Dokumente stehen in der Bibliothek von *Tivoli Remote Control* zur Verfügung:

- *IBM Tivoli Remote Control: Benutzerhandbuch*, SC12-3220

  Enthält Informationen zu Tivoli Remote Control-Konzepten und zur Installation und Verwendung von Tivoli Remote Control.
- *IBM Tivoli Remote Control: Messages and Codes*, SC23-4843

  Enthält Informationen zu Tivoli Remote Control-Nachrichten.
- *IBM Tivoli Remote Control: Release-Notes*, SC12-3221

  Enthält aktuelle Informationen zu Tivoli Remote Control und eine Liste mit bereits behobenen und noch zu lösenden Problemen des Produkts und der Dokumentation.
- *IBM Tivoli Remote Control: Read This First*, SC09-7794

  Enthält Informationen zum Inhalt der CD-ROMs von Tivoli Remote Control.

Vorausgesetzte Literatur

Um die Informationen in diesem Handbuch effektiv nutzen zu können, sind einige Vorkenntnisse erforderlich, die Sie folgenden Büchern entnehmen können:

- *Tivoli Management Framework: Firewall Security Toolbox User's Guide*, GC23-4826

  Bietet Lösungen zum Management Ihres Tivoli-Netzwerks über Firewalls, ohne dabei die Sicherheit zu gefährden.
- *Tivoli Management Framework: Benutzerhandbuch*, GC12-3134, *Tivoli Management Framework: Reference Manual*, GC32-0806

  Enthält ausführliche Informationen zur Vorgehensweise beim Management der Tivoli-Umgebung über den Tivoli-Desktop oder die Befehlszeile.
- *Tivoli Enterprise Console: Benutzerhandbuch*, GC12-2743

  Enthält ausführliche Informationen zur Integration von Netzwerken, Systemen und Datenbanken und zum Anwendungsmanagement mit Tivoli Enterprise Console.

Referenzliteratur

Das *Tivoli-Glossar* enthält die Definitionen vieler Fachbegriffe, die sich auf Tivoli-Software beziehen. Das *Tivoli-Glossar* ist auf folgender Website, allerdings nur in Englisch, verfügbar:

http://www.tivoli.com/support/documents/glossary/termsm03.htm

Online-Veröffentlichungen

Veröffentlichungen in den Produktbibliotheken befinden sich im PDF-Format auf der Produkt-CD. Um auf diese Veröffentlichungen über einen Web-Browser Zugriff zu erhalten, öffnen Sie die Datei 'infocenter.htm' auf der CD mit der Produktdokumentation.

Von IBM aktualisierte Versionen von Online- und Hardcopy-Veröffentlichungen werden im Tivoli Information Center veröffentlicht. Auf die aktualisierten Veröffentlichungen im Tivoli Information Center können Sie über folgende Website für die IBM Kundenunterstützung zugreifen:

http://www.tivoli.com/support/documents/

Das Tivoli Information Center enthält die neusten Versionen der Bücher in der Produktbibliothek im PDF- und/oder HTML-Format. Ein Teil dieser Dokumentation liegt in mehreren Sprachen vor.

Anmerkung: Wenn Sie PDF-Dokumente auf Papier mit einem anderen Format als 'Letter' drucken möchten, aktivieren Sie im Adobe Acrobat-Dialog 'Drucken' die Option zum Einpassen in die Seitengröße (verfügbar, wenn Sie auf **Datei --> Drucken** klicken), um sicherzustellen, dass der vollständige Inhalt einer Seite in Letter-Größe auf dem von Ihnen verwendeten Papier ausgedruckt wird.

Veröffentlichungen bestellen

Viele Tivoli-Veröffentlichungen können Sie online auf der folgenden Website bestellen:

http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi

Die Bestellung kann auch per E-Mail, Telefon oder Fax erfolgen:

- Telefon: +49 180 55090 bzw. 0180 55090
- Fax: 07032 15 3300
- E-Mail: LITERATA@DE.IBM.COM
- Eine Liste mit Telefonnummern in anderen Ländern finden Sie auf folgender Website: http://www.tivoli.com/inside/store/lit_order.html

Rückmeldungen zu Veröffentlichungen

Bitte teilen Sie uns mit, welche Erfahrungen Sie mit Produkten und Dokumentationen von Tivoli gemacht haben. Wir freuen uns über Ihre Kommentare und Verbesserungsvorschläge, die Sie uns auf einem der folgenden Wege mitteilen können:

- Senden Sie eine E-mail an pubs@tivoli.com.
- Beteiligen Sie sich an unserer Kundenumfrage im Internet unter: http://www.tivoli.com/support/survey/

Eingabehilfen

Die Funktionen der Eingabehilfe ermöglichen Benutzern mit körperlichen Behinderungen (z. B. mit eingeschränkter Beweglichkeit oder eingeschränktem Sehvermögen) die effektive Nutzung von Softwareprodukten. Dieses Produkt bietet Unterstützungstechnologien zur Bildschirmsprachausgabe und Navigation der Benutzerschnittstelle. Alle Funktionen der grafischen Benutzerschnittstelle können auch über die Tastatur statt über die Maus aufgerufen werden.

Weitere Informationen hierzu finden Sie in Anhang A, „Eingabehilfen", auf Seite 137.

Kundenunterstützung anfordern

Wenn Sie Probleme mit einem Tivoli-Produkt haben, können Sie sich an die Kundenunterstützung wenden. Siehe das *Customer Support Handbook* auf folgender Website:

http://www.tivoli.com/support/handbook/

Dieses Buch enthält neben Informationen zur Kontaktaufnahme mit der Kundenunterstützung je nach Schwere des Problems auch folgende Informationen:

- Registrierung und Nutzungsberechtigung
- Telefonnummern und E-Mail-Adressen für das Land, in dem Sie sich befinden
- Informationen, die Sie vor der Kontaktaufnahme mit der Kundenunterstützung zusammenstellen sollten

In diesem Handbuch verwendete Konventionen

In diesem Handbuch werden verschiedene Konventionen für bestimmte Begriffe und Aktionen, betriebssystemabhängige Befehle und Pfade verwendet.

Schriftbildkonventionen

Folgende Schriftbildkonventionen werden in diesem Handbuch verwendet:

Fett Befehle in Kleinschreibung sowie in gemischter Groß- und Kleinschreibung, Befehlsoptionen und Kennungen werden im Text in **Fettdruck** dargestellt.

Elemente der grafischen Benutzerschnittstelle (mit Ausnahme von manchen Fenster- und Dialogtiteln) und Tastennamen werden ebenfalls in **Fettdruck** dargestellt.

Kursiv Variablen, Werte, die vom Benutzer eingegeben werden müssen, neue Begriffe sowie Wörter und Ausdrücke, die hervorgehoben werden sollen, werden *kursiv* dargestellt.

`Monospace-Schrift`
Befehle, Befehlsoptionen und Kennungen, die in einer eigenen Zeile aufgeführt werden, Codebeispiele, Ausgaben- und Nachrichtentexte werden in `Monospace-Schrift` dargestellt.

Datei- und Verzeichnisnamen, Zeichenfolgen, die vom Benutzer eingegeben werden müssen, sofern sie im Text angegeben werden, Namen von Java-Methoden und -Klassen sowie HTML- und XML-Tags werden ebenfalls in `Monospace-Schrift` dargestellt.

Betriebssystemabhängige Variablen und Pfade

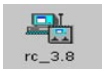
Im vorliegenden Buch werden für die Angabe von Umgebungsvariablen und Verzeichnissen die Windows-Konventionen verwendet.

Wenn Sie die UNIX-Befehlszeile verwenden, müssen Sie daher für Umgebungsvariablen die Angabe %*variable*% durch $*variable* und in Verzeichnispfaden jeden umgekehrten Schrägstrich (\) durch einen Schrägstrich (/) ersetzen.

Anmerkung: Wenn Sie auf einem Windows-System mit der Bash-Shell arbeiten, können Sie die UNIX-Konventionen verwenden.

Symbol für Tivoli Remote Control

Das folgende Symbol steht für das Tivoli Remote Control-Tool:



Das Remote Control-Tool wird in einem Richtlinienbereich erstellt. Es ermöglicht die Ausführung von fernen Operationen wie beispielsweise die Fernsteuerung bzw. den Neustart einer Workstation, die Übertragung von Dateien und das Chatten.

Kapitel 1. Übersicht zu Tivoli Remote Control

Tivoli Remote Control unterstützt Sie bei der Verwaltung von Workstations in einem Netzwerk. Mit Hilfe von Tivoli Remote Control können Sie von einer zentralen Stelle aus Workstations an fernen Standorten überwachen und steuern.

Vor der Installation der Tools sollten einige Sicherheitsaspekte bedacht werden. Diese Aspekte werden unter „Steuerung der Tivoli Remote Control-Sicherheit" auf Seite 2 näher erläutert.

Funktionen in Tivoli Remote Control

Bei der Arbeit mit Tivoli Remote Control wird die Workstation des Administrators als ***Controller*** bezeichnet. Die fernen Workstations werden als ***Ziele*** bezeichnet. Folgende Funktionen können vom Controller aus ausgeführt werden:

- Anzeige eines Ziels überwachen. Siehe „Aktion 'Remote Control' verwenden" auf Seite 101.
- Eingaben über die Tastatur oder Maus vom Controller aus tätigen und so das Ziel steuern. Siehe „Aktion 'Remote Control' verwenden" auf Seite 101.
- Neustart eines Ziels ausführen. Siehe „Aktion 'Neustart' verwenden" auf Seite 106.
- Schriftlichen Dialog mit einem Ziel führen. Siehe Kapitel 10, „Aktion 'Chat' verwenden", auf Seite 107.
- Dateien oder Verzeichnisse zwischen Controller und Ziel übertragen. Siehe Kapitel 11, „Aktion 'Dateiübertragung' verwenden", auf Seite 113.
- Tivoli Remote Control in einer Terminal-Server-Umgebung ausführen.
- Ferne Operationen über Firewalls ausführen. Dies gilt jedoch nicht für die Aktion 'Chat'.

Der Zeitraum zwischen dem Start einer Aktion und dem Beenden dieser Aktion wird als *Sitzung* bezeichnet.

Komponenten von Tivoli Remote Control

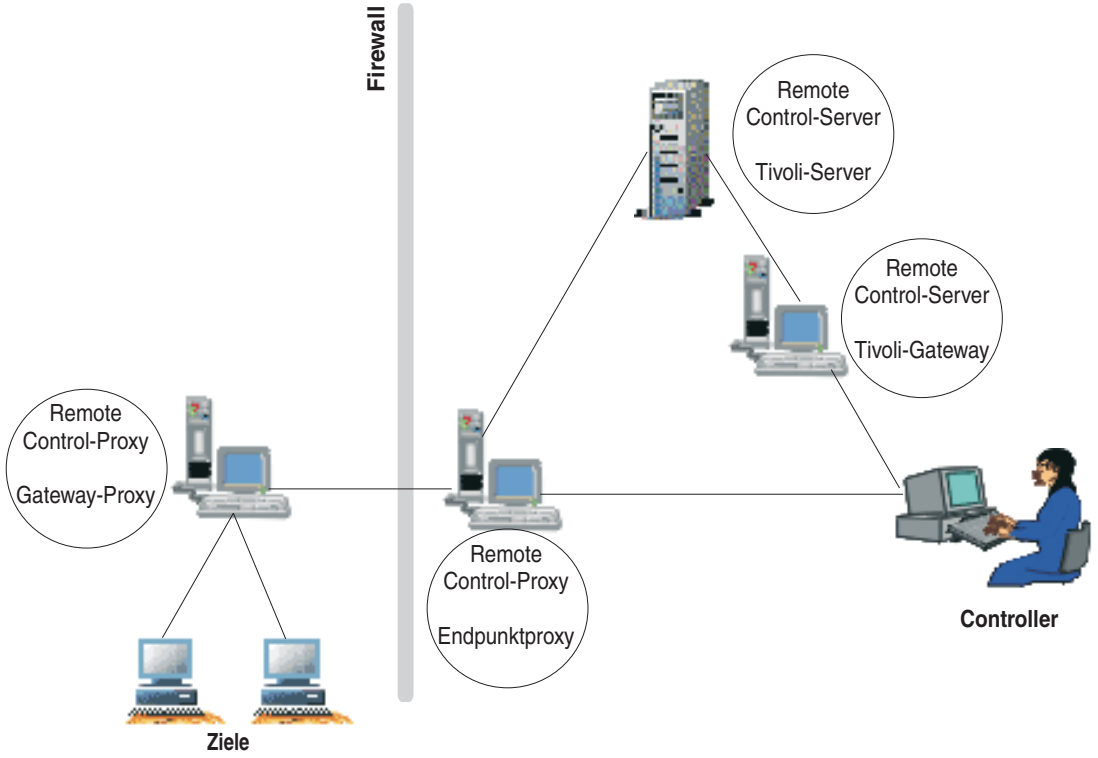
Tivoli Remote Control ist eine Client/Server-Anwendung. Sie besteht aus folgenden fünf Hauptkomponenten:

- ***Remote Control-Server***. Dieser Server stellt die Funktionen von Tivoli Remote Control bereit. Der Server muss auf einem verwalteten Knoten installiert sein.
- ***Controller*** (die Workstation Ihres Administrators). Darauf wird Client-Software ausgeführt, die Funktionen vom Server anfordert. Controller müssen Endpunkte sein.
- ***Ziel*** (die Workstation des Benutzers). Darauf wird Client-Software ausgeführt, die Funktionen vom Server anfordert. Ziele müssen Endpunkte sein. Frühere Versionen (3.7.1) des Zielclients werden jedoch von der Version 3.8 des Servers unterstützt.
- ***Remote Control-Proxy***. Hierbei handelt es sich um eine optionale Komponente, die die Kommunikation zwischen Controllern und Zielen über Firewalls vereinfacht.

- ***Remote Control-Gateway***. Dies ist eine optionale frühere Komponente, die die Kommunikation zwischen Controllern und Zielrechnern steuert, wenn diese nicht direkt miteinander kommunizieren.

Weitere Informationen zu verwalteten Knoten und Endpunkten finden Sie in den Handbüchern *Tivoli Management Framework Planung und Installation* sowie *Tivoli Management Framework Benutzerhandbuch*.

Das folgende Beispiel zeigt eine typische Konfiguration. Mit einem Controller werden die Zielrechner überwacht. Die Remote Conrol-Proxys ermöglichen die Kommunikation über Firewalls.



Steuerung der Tivoli Remote Control-Sicherheit

In Tivoli Remote Control stehen folgende Sicherheitsstufen zur Verfügung:

- „Berechtigungsklassen"
- „Standardrichtlinie" auf Seite 3
- „Generierung von Hinweisen" auf Seite 3
- „Generierung von Protokollen und Traces" auf Seite 3
- „Datenverschlüsselung" auf Seite 4
- „Aktivierung der Firewall" auf Seite 4

Berechtigungsklassen

Die Berechtigungsklassen regeln den grundlegenden Zugriff auf Aktionen in Tivoli Remote Control. Tivoli Remote Control stellt eindeutige Berechtigungsklassen zur Verfügung, die nicht hierarchisch sind. Aus diesem Grund muss ein Administrator allen Tivoli Remote Control-Berechtigungsklassen explizit zugeordnet werden, damit er die Tasks, die den Berechtigungsklassen zugeordnet sind, ausführen kann.

Sie können wie folgt zugeordnet werden:

- In dem Richtlinienbereich, zu dem das Zielsystem gehört.
- In der gesamten Tivoli Management Region.

Weitere Informationen finden Sie unter „Schritt 3: Tivoli Remote Control-Berechtigungsklassen zuordnen" auf Seite 69.

Standardrichtlinie

Bei der Standardrichtlinie handelt es sich um eine Gruppe von Merkmalwerten für Ressourcen, die einer Ressource zugeordnet wird, wenn diese erstellt wird. Die Standardrichtlinie definiert die Richtlinienmethoden, die einem Remote Control-Tool zugeordnet sind. Auf diese Weise wird das Verhalten der Tivoli Remote Control-Aktionen gesteuert. Die Standardrichtlinie kann in Übereinstimmung mit Ihrem Sicherheitsmodell konfiguriert werden. Beispiel:

- Sie können alle Administratoren dazu berechtigen, sämtliche in Tivoli Remote Control verfügbaren Funktionen auszuführen.
- Als Administrator mit der Berechtigungsklasse 'senior' können Sie die Standardrichtlinie bearbeiten, um die Verwendung der Remote Control-Tools einzuschränken.

Die Steuerungsmöglichkeiten eines Administrators können mit Hilfe der Methoden begrenzt werden, die der Standardrichtlinie zugeordnet sind. Weitere Informationen finden Sie unter Kapitel 6, „Standardeinstellungen des Remote Control-Tools ändern", auf Seite 71.

Generierung von Hinweisen

Tivoli Remote Control verwendet die Hinweise als Prüfliste für wichtige Operationen, die von Ihnen ausgeführt werden. Über das Symbol 'Hinweise' auf dem Tivoli-Desktop können Sie auf die Hinweise zugreifen.

In Tivoli Remote Control wird für folgende Ereignisse ein Hinweis generiert:

- Start und Ende einer Sitzung.
- Fehlerhafte Sitzung.

Der Hinweis enthält auch Informationen zum Ergebnis einer Operation (Hinweis, Warnung oder Fehler), zum verantwortlichen Administrator, und je nach Art des Ereignisses die Controllerkennung, die Zielkennung und die für die Sitzung ausgewählten Optionen wie beispielsweise Reaktionszeit, Aktion bei Zeitlimitüberschreitung, Anfangsstatus, Änderungsstatus. Diese Informationen werden standardmäßig an die Tivoli Remote Control-Hinweisgruppe gesendet.

Generierung von Protokollen und Traces

Tivoli Remote Control-Operationen können in Protokoll- und Tracedateien aufgezeichnet werden. Protokolldateien können für Prüf- und Debugvorgänge verwendet werden, während Tracedateien ausschließlich für Debugvorgänge verwendet werden.

Datenverschlüsselung

Sie können alle Daten, die während einer Remote Control-Sitzung bzw. einer Dateiübertragungs-Sitzung zwischen einem Controller und einem Zielrechner ausgetauscht werden, verschlüsseln. Zur Verschlüsselung von Daten verwendet Tivoli Remote Control den 3DES-Verschlüsselungsalgorithmus. Die privaten Schlüssel werden unter Verwendung des Diffie-Hellmann-Schlüsselaustauschprotokolls generiert und ausgetauscht. Weitere Informationen zur Definition von Datenverschlüsselung finden Sie unter „rc_def_encryption" auf Seite 77.

Aktivierung der Firewall

Sie können Tivoli Remote Control in einer Netzwerkumgebung mit Firewalls verwenden. Mit Hilfe des Remote Control-Proxys, der neuen Komponente von Tivoli Remote Control, können mehrere Maschinen auf einer Seite einer Firewall über einen gemeinsamen definierbaren Port mit mehreren Maschinen, die sich auf der anderen Seite der Firewall befinden, kommunizieren. Auf diese Weise kann ein beliebiger Controller auf einer Seite einer Firewall (oder einer Reihe von Firewalls) mit einem Zielrechner, der sich auf der anderen Seite der Firewall (oder einer Reihe von Firewalls) befindet, unter Berücksichtigung der geltenden Einschränkungen eine Sitzung starten.

Neue Funktionen in Tivoli Remote Control Version 3.8

Mit Tivoli Remote Control Version 3.8 haben Sie folgende Möglichkeiten:

- Sie können alle Daten, die während einer Remote Control-Sitzung bzw. einer Dateiübertragungs-Sitzung ausgetauscht werden, verschlüsseln.
- Sie können sichere Sitzungen über Firewalls ausführen. Dies gilt jedoch nicht für Chat-Sitzungen.
- Sie können für die meisten Remote Control-Operationen Protokolle und Traces generieren.
- Sie können mit einer effektiveren Webschnittstelle arbeiten.
- Sie können den Tivoli Remote Control-Server und die Proxykomponenten von Remote Control auf Linux-Plattformen ausführen.
- Sie können die Prüffunktion verbessern.
- Sie können Tivoli Remote Control in traditionellem Chinesisch verwenden.
- Sie können die NAT-Funktionen nutzen.
- Sie können die Leistung verbessern.
- Sie können den Controller und das Ziel mit dem Befehl **wrcuninstep** deinstallieren.

Kapitel 2. Planung und Installation von Tivoli Remote Control

Dieses Kapitel enthält Hinweise zur Planung und Installation der entsprechenden Komponenten von Tivoli Remote Control. Folgende Informationen sind in diesem Kapitel enthalten:

- Eine Liste mit Tasks und Prüfvorgängen, die Sie durchführen müssen, bevor Sie die Installation von oder einen Upgrade auf Tivoli Remote Control 3.8 starten. Siehe „Einführung" auf Seite 5.
- Informationen zu Hardware- und Softwarevoraussetzungen und den erforderlichen Benutzerberechtigungen. Siehe „Voraussetzungen" auf Seite 6.
- Informationen zu den Komponenten von Tivoli Remote Control Version 3.8 und dem Systemtyp, auf dem die jeweiligen Komponenten installiert werden müssen. Siehe „Komponenten, unterstützte Betriebssysteme und Protokolle" auf Seite 10.
- Informationen zur Planung Ihrer Tivoli Remote Control-Umgebung und zur Installation der Anwendung mit verschiedenen Installationsmethoden. Siehe „Tivoli Remote Control installieren" auf Seite 9.
- Informationen für den Upgrade auf Tivoli Remote Control Version 3.8 unter Anwendung verschiedener Installationsmethoden. Siehe „Upgrades von früheren Releases" auf Seite 17.
- Anweisungen für das Entfernen von Tivoli Remote Control Version 3.8. Siehe „Tivoli Remote Control deinstallieren" auf Seite 22.

In den *IBM Tivoli Remote Control: Release-Notes* finden Sie aktuelle Informationen zu den Systemvoraussetzungen, Änderungen am Installationsverfahren und Lösungen für bekannte Probleme.

Einführung

Bevor Sie eine Installation bzw. einen Upgrade auf Tivoli Remote Control Version 3.8 ausführen, führen Sie folgende Schritte aus:

- Sie sollten vor der Installation von Tivoli Remote Control für alle Maschinen in der Tivoli Management Region (TMR) eine Sicherungskopie Ihrer Tivoli Management Framework-Datenbank erstellen. Mit Hilfe der Sicherungskopien können Sie zu dem Status der Datenbank vor der Installation zurückkehren, wenn bei der Installation von Tivoli Remote Control Probleme auftreten. Um eine Sicherungskopie des Tivoli-Servers und der verwalteten Knoten in Tivoli zu erstellen, wählen Sie auf dem Tivoli-Desktop die Optionen **Desktop → Sichern** aus, oder verwenden Sie den Befehl **wbkupdb**. Weitere Informationen zum Befehl **wbkupdb** finden Sie im Handbuch *Tivoli Management Framework Reference Guide*.
- Stellen Sie sicher, dass der Server, die verwalteten Knoten und Endpunkte, auf denen die Komponenten von Tivoli Remote Control Version 3.8 installiert werden sollen, die Hardware- und Softwarevoraussetzungen für das Produkt erfüllen.
- Stellen Sie sicher, dass die Endpunkte, auf denen Sie Tivoli Remote Control installieren möchten, den entsprechenden Gateways mit einem vollständig qualifizierten Namen bzw. einer IP-Adresse zugeordnet sind.

Vor der Installation

- Lesen Sie den Abschnitt „Komponenten, unterstützte Betriebssysteme und Protokolle" auf Seite 10 und entscheiden Sie, welche Komponenten Sie auf welchen Systemen installieren möchten.
- Stellen Sie sicher, dass keine anderen Softwareprogramme zur Fernsteuerung installiert sind, da Tivoli Remote Control nicht mit diesen zusammen ausgeführt werden kann.

Voraussetzungen

Wenn Sie Tivoli Remote Control zum ersten Mal installieren, sollten Sie überprüfen, ob die Hardware und Software den in diesem Abschnitt angegebenen Anforderungen entsprechen oder diese sogar überschreiten.

Informationen zu den Dateien, die bei der Installation geändert werden, finden Sie im Anhang C, „Bei der Installation geänderte Registrierungsdatenbanken und Dateien", auf Seite 145.

Hardwarevoraussetzungen

Für Tivoli Remote Control bestehen bestimmte Hardwarevoraussetzungen, die erfüllt sein müssen, damit das Produkt installiert und ordnungsgemäß funktionieren kann. Diese Anforderungen beziehen sich auf Hardwareplattformen, den Arbeitsspeicher und den Festplattenspeicherplatz. Die nachfolgend aufgelisteten Voraussetzungen für die Umgebung von Tivoli Remote Control werden derzeit empfohlen. Tivoli Remote Control wird nur dann unterstützt, wenn das Produkt unter Voraussetzungen ausgeführt wird, die von Fremdanbietern offiziell bereitgestellt werden.

Unterstützte Hardwareplattformen

In der nachfolgenden Tabelle werden die unterstützten Betriebssystemversionen für die jeweiligen unterstützten Hardwareplattformen aufgeführt.

Betriebssystem	Unterstützte Hardwareplattform
AIX®	pSeries™- und PowerPC®-Systeme im 32-Bit-Modus mit AIX Version 4.3.3 und 5.1
HP-UX	HP9000/700- und -800-Serie mit HP-UX, Versionen 11.0 und 11i.
Linux for Intel®	Intel- oder Pentium®-Systeme mit Red Hat 7.2, SuSE 7.3 oder TurboLinux 6.5
Linux for S/390®	IBM S/390 G5-, G6-, oder MP3000-System mit Red Hat 7.2 on zSeries, SuSE Enterprise Server 7.0 on zSeries
OS/2	Intel- oder Pentium-Systeme mit IBM OS/2 Warp Server 4.5.1 und Warp Server for E-Biz 4.5.
Solaris-Betriebsumgebung	Sun SPARC-Serie mit Solaris-Betriebsumgebung Version 7 und 8.
Windows	Intel- oder Pentium-Systeme mit Windows 98 Second Edition.
Windows NT	Intel- oder Pentium-Systeme mit Microsoft® Windows NT Version 4.0 SP6A, Windows NT Terminal Server Edition+SP4 oder höher.
Windows 2000	Intel- oder Pentium-Systeme mit Microsoft Windows 2000.
Windows XP	Intel- oder Pentium-Systeme mit Microsoft Windows XP.

Voraussetzungen bezüglich des Arbeitsspeichers

Ihre Workstation muss über mindestens 64 MB RAM verfügen, um Tivoli Remote Control ausführen zu können.

Voraussetzungen bezüglich des Festplattenspeichers

In den folgenden Tabellen ist der erforderliche Festplattenspeicher für die jeweiligen Betriebssystemkonfigurationen aufgeführt, der für Zielmaschine, Controller, Server und Proxy von Tivoli Remote Control erforderlich ist.

Um den erforderlichen Festplattenspeicher für die Installation der Software zur Dateiübertragung und der Chat-Software zu ermitteln, müssen Sie auch den Speicherplatz berücksichtigen, der von den Dateien von Java™ Run-time Environment 1.3 belegt wird. Falls diese Dateien noch nicht vorhanden sind, werden sie beim Start einer Sitzung zur Dateiübertragung bzw. Chat-Sitzung heruntergeladen.

Software für Tivoli Remote Control	**Erforderlicher Festplattenspeicher (in MB)**						
	Windows 98 Second Edition	**Windows XP**	**Windows NT**	**Windows 2000**	**UNIX/Linux for Intel**	**Linux for S/390**	**OS/2**
Remote Control-Controller	1,5	1,9	1,8	1,8		-	1,1
Remote Control-Zielrechner	0,8	2,7	2,7	2,7	-	-	1,3
Tivoli Remote Control-Server/-Gateway	-	-	-	57,3	57,3	-	-
Dateiübertragungs-Controller	1,8	1,8	1,8	1,8	-	-	1,8
Dateiübertragungs-Zielmaschine	1,7	1,7	1,7	1,7	-	-	1,7
Chat, Controller	0,7	0,7	0,7	0,7	-	-	0.7
Chat, Zielmaschine	0,7	0,7	0,7	0,7	-	-	0,7
JRE 1.3	24	24	24	24	-	-	24,8

Software für Tivoli Remote Control	**Erforderlicher Festplattenspeicher (in MB)**			
	Windows 2000	**AIX**	**Linux for Intel**	**Solaris-Betriebsumgebung**
Tivoli Remote Control-Proxy	28,3	32,1	35,7	57,8

Ausführliche und aktuelle Informationen finden Sie im Handbuch *IBM Tivoli Remote Control: Release-Notes*.

Softwarevoraussetzungen

Tivoli Remote Control kann nicht zusammen mit anderen Softwareprogrammen zur Fernsteuerung ausgeführt werden.

Vor der Installation von Tivoli Remote Control muss folgende Software bereits installiert sein und ausgeführt werden:

- Ein unterstütztes Betriebssystem und Netzwerkprotokoll.
- Tivoli Management Framework 3.7.1 oder höher.

Zusätzliche Anforderungen:

- Der Tivoli-Managementagent von Tivoli Management Framework Version 3.7.1 oder höher (LCF-Version 91 oder höher) muss auf den Workstations, die als Controller und Zielrechner fungieren, installiert sein.
- Der Tivoli-Desktop muss auf den Workstations installiert sein, auf denen Sie die grafische Benutzerschnittstelle von Tivoli Remote Control verwenden möchten.
- Einer der folgenden Web-Browser muss auf den Workstations installiert sein, auf denen Sie die die Webschnittstelle von Tivoli Remote Control nutzen möchten:
  - Netscape 4.6 oder höher
  - Internet Explorer 5.0 oder 5.5+SP1
- IBM Tivoli Firewall Security Toolbox 1.3 oder höher muss installiert sein, wenn der Remote Control-Proxy nicht im Standalone-Modus verwendet werden soll.

Erforderliche Benutzerberechtigungen auf Windows-Endpunkten

Um Tivoli Remote Control auf Windows NT-, Windows 2000- und Windows XP-Endpunkten ausführen zu können, müssen Sie sicherstellen, dass Sie über die in den folgenden Abschnitten beschriebenen Benutzerberechtigungen verfügen.

Schritt 1: Tivoli Remote Control installieren und Sitzung starten

Bevor Sie Tivoli Remote Control installieren und eine Sitzung starten, müssen Sie sicherstellen, dass es sich bei dem für die Zuordnungsvariable *root_user* angegebenen Benutzerkonto um ein Administratorenkonto für das Betriebssystem des Endpunkts handelt. Die Zuordnungsvariable *root_user* ist in der Tivoli Management Region (TMR) definiert. Sie können die zugehörigen Werte mit dem Befehl **widmap** überprüfen, um einen Endpunkt in einem Richtlinienbereich zu definieren.

Bei Windows NT-, Windows 2000- und Windows XP-Endpunkten ist der Standardwert für die Zuordnungsvariable *root_user* das integrierte Standardkonto des Administrators (z. B. **Administrator** auf englischen Maschinen). Wenn Sie das **integrierte, standardmäßige Administratorenkonto** umbenennen oder ein anderen Windows-Kontonamen für die Zuordnungsvariable *root_user* verwenden, müssen Sie sicherstellen, dass das neue Benutzerkonto folgende Konventionen erfüllt:

- Es ist entweder auf Domänenebene oder auf allen Endpunkten in der Tivoli Management Region (TMR) definiert.

  Anmerkung: Wenn Sie mit Tivoli Management Framework arbeiten und das integrierte Administratorenkonto auf einigen Endpunkten umbenannt haben, können Sie für den Wert *root_user* **BuiltinNTAdministrator** einsetzen. Auf diese Weise können Sie Tivoli Remote Control auf jedem beliebigen Endpunkt eines Tivoli-Bereichs installieren

und eine Sitzung starten, selbst wenn die Namen für das integrierte Administratorenkonto auf den jeweiligen Endpunkten nicht identisch sind.

- Es ist auf allen Endpunkten in den Gruppen 'Windows Administrators' und 'Tivoli_Admin_Privileges' definiert.
- Es verfügt über eine Berechtigung zur vollständigen Steuerung der folgenden Verzeichnisse:
  - `%WINDIR%`
  - `%WINDIR%\system32`
  - `%WINDIR%\system32\drivers`
  - `%LCF_DIR%`
- Es verfügt über eine vollständige Zugriffsberechtigung für die folgenden Registrierungsschlüssel:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
  HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli
  ```

- Unter dem Benutzerkonto können folgende Vorgänge ausgeführt werden:
  - Lokal anmelden
  - Auf die Workstation vom Netzwerk aus zugreifen
  - Services und Driver installieren
  - Neustart der Workstation durchführen

Schritt 2: Eine Sitzung ausführen

Nachdem eine Sitzung gestartet wurde, wird Tivoli Remote Control unter dem vordefinierten lokalen Windows-Konto **System** ausgeführt, das über zahlreiche Berechtigungen für die lokale Maschine verfügt. Wenn Sie die Berechtigungen dieses Kontos ändern, müssen Sie sicherstellen, dass es zumindest die folgenden Konventionen für die jeweiligen Windows-Betriebssysteme der Endpunkte erfüllt:

- Es verfügt über eine Berechtigung zur kompletten Steuerung der folgenden Verzeichnisse:
  - `%WINDIR%`
  - `%WINDIR%\system32`
  - `%WINDIR%\system32\drivers`
  - `%LCF_DIR%`
- Es verfügt über eine vollständige Zugriffsberechtigung für alle Registrierungsschlüssel.
- Lokale Anmeldung ist zulässig.

Tivoli Remote Control installieren

Um Tivoli Remote Control in einem Bereich zu installieren, müssen Sie folgende Schritte ausführen:

1. Installieren Sie den Tivoli Remote Control-Server zunächst auf dem Tivoli-Server und anschließend auf
   - den Tivoli-Gateways, die mit den Endpunkten verbunden sind, auf denen Sie Controller und Ziele installieren möchten.
   - auf den verwalteten Knoten, die als Remote Control-Gateway fungieren sollen.
   - auf den verwalteten Knoten, auf denen das Remote Control-Tool ausgeführt werden soll.

Weitere Informationen finden Sie unter „Schritt 1: Tivoli Remote Control-Server auf verwalteten Knoten installieren" auf Seite 12.

2. Installieren Sie Controller und Ziele auf den Endpunkten. Diese Komponenten werden an Endpunkte verteilt, wenn Sie eine Tivoli Remote Control-Aktion zwischen diesen Endpunkten zum ersten Mal starten. Weitere Informationen finden Sie unter „Schritt 2: Controller und Ziele auf Endpunkten installieren" auf Seite 14.
3. Installieren Sie das Remote Control-Gateway auf den verwalteten Knoten (optional). Installieren Sie hierzu den Remote Control-Server und konfigurieren Sie diesen als Remote Control-Gateway. Weitere Informationen finden Sie unter „Schritt 3: Das Tivoli Remote Control-Gateway auf verwalteten Knoten installieren" auf Seite 16.
4. Installieren Sie Remote Control-Proxys, wenn Sie eine Sitzung über Firewalls ausführen müssen. Je nach Position der Firewall müssen Sie den Remote Control-Proxy entweder auf den Workstations mit dem Endpunktproxy und dem Gateway-Proxy installieren, oder auf zwei anderen Workstations. Weitere Informationen finden Sie unter Kapitel 3, „Sitzungen über Firewalls ausführen", auf Seite 25.

Informationen zur Installation eines Upgrades auf der Basis einer älteren Version finden Sie unter „Upgrades von früheren Releases" auf Seite 17.

Komponenten, unterstützte Betriebssysteme und Protokolle

In der folgenden Tabelle sind die indexierten Dateien, Komponenten und Produktkennungen aufgeführt, die zur Identifikation der zu installierenden Komponente herangezogen werden.

Indexierte Datei	Komponentenname	Produktkennung
RC_ALI	Tivoli Remote Control Server 3.8	RC_ALI

- Die indexierte Datei wird zur Installation der Komponente mit dem Befehl **winstall** verwendet.
- Der Komponentenname wird verwendet, wenn die Komponente über den Tivoli-Desktop oder die SIS-Konsole installiert wird.
- Die Produktkennung wird verwendet, wenn die Komponente mit dem Befehl **wuninst** deinstalliert wird.

Die Installationsimages befinden sich in den folgenden Verzeichnissen der IBM Tivoli Remote Control-CD.

Images	CD-Verzeichnis
Tivoli Remote Control Server 3.8	new\RC
Tivoli Remote Control Proxy	new\RCPROXY
Tivoli Remote Control Server 3.8 Upgrade	upgrade\RC

In der folgenden Tabelle werden die Komponenten von Tivoli Remote Control aufgelistet, die von den verschiedenen Betriebssystemen unterstützt werden:

Betriebssystem	Version	Server, Gateway	Proxy	Controller	Ziel
AIX	4.3.3 5.1	✓	✓		

Betriebssystem	Version	Server, Gateway	Proxy	Controller	Ziel
Solaris-Betriebsumgebung	7 8	✓	✓		
HP-UX	11.0 11i	✓			
Red Hat Linux Server	7.1 7.2	✓	✓		
Red Hat Linux for S/390	7.2	✓			
SuSE Linux	7.3	✓	✓		
TurboLinux	6.5	✓	✓		
Suse Linux Enterprise Server for zSeries and S/390	7	✓			
Windows 2000	Professional oder höher			✓	✓
	Server oder höher	✓	✓	✓	✓
	Advanced Server oder höher	✓	✓	✓	✓
Windows NT	4.0 + SP 6A			✓	✓
	4.0 Terminal Server Edition oder höher			✓	
Windows 98	Second Edition			✓	✓
Windows XP	Professional			✓	✓
OS/2 Warp Server	4.5.1			✓	✓
OS/2 Warp Server for E-Biz	4.5			✓	✓

Anmerkung: Bei der Installation des Remote Control-Proxys müssen Sie folgendes sicherstellen:

- Der verfügbare Speicherplatz im Dateisystem '/tmp' beträgt 48 MB.
- Sie haben das AIX-Paket mit Wartungsstufe AIX 4330-02 unter AIX 4.3.3.0 installiert.
- Sie haben die für die Ausführung von JRE 1.3 in der Solaris-Betriebsumgebung 7 und 8 erforderlichen Programmkorrekturen installiert. Weitere Informationen zu den erforderlichen Programmkorrekturen finden Sie auf folgender Website:

  http://java.sun.com/j2se/1.3/install-solaris-patches.html

Sie können von Controllern eine Verbindung zu Zielrechnern mit jedem der folgenden Betriebssysteme herstellen, vorausgesetzt, auf den Zielrechnern und den Controllern sind die entsprechenden Protokolle installiert.

Betriebssystem	Protokoll
OS/2 Warp Server 4.5.1 oder höher, für Systeme mit Einzelbytezeichensatz	IBM TCP/IP 4.2 for OS/2 oder höher
OS/2 Warp Server for E-Biz 4.5	
Windows 2000, Windows NT, Windows XP, Windows 98 Second Edition	Integrierter TCP/IP-Stack

Weitere Informationen zum unterstützten TCP/IP-Stack (TCP/IP-Stapel) finden Sie in den *Tivoli Management Framework Release Notes*.

Schritt 1: Tivoli Remote Control-Server auf verwalteten Knoten installieren

Für die Installation des Remote Control-Servers stehen Ihnen folgende Methoden zur Verfügung:

- Mit Tivoli Software Installation Service (SIS). Siehe „Tivoli Software Installation Service (SIS) verwenden".
- Über den Tivoli-Desktop. Weitere Informationen finden Sie unter „Über den Tivoli-Desktop".
- Mit dem Befehl **winstall**. Weitere Informationen finden Sie unter „Den Befehl 'winstall' verwenden" auf Seite 13.

Tivoli Software Installation Service (SIS) verwenden

Mit dem Tivoli Software Installation Service (SIS) können Sie mehrere Tivoli-Produkte auf mehreren Systemen gleichzeitig installieren. Mit diesem Java-basierten Produkt können Sie mehrere Produkte auf mehreren Systemen sehr viel schneller als mit dem Installationsprogramm von Tivoli Management Framework installieren.

Vor der Installation des Remote Control-Servers unter Verwendung von SIS müssen Sie sicherstellen, dass die Programmkorrekturen '3.7-SIS-DEPOT-0005' und '3.7-SISCLNT-0005' installiert wurden.

Gehen Sie bei der Installation des Remote Control-Servers unter Verwendung von SIS wie folgt vor:

1. Importieren Sie die Produktimages in das SIS-Depot.
2. Wählen Sie die Serverkomponente von Remote Control aus.
3. Wählen Sie die Maschinen aus, auf denen die jeweiligen Komponenten installiert werden sollen.
4. Klicken Sie auf **Installieren**.

Geben Sie auf den Tivoli-Gateways, auf denen Sie den Remote Control-Server installiert haben, in der Eingabeaufforderung folgendes ein:

```
wgateway <Gatewaykennung> restart
```

Weitere Informationen zur Verwendung von SIS zur Installation der Komponenten finden Sie im Handbuch *Tivoli Software Installation Service User's Guide*.

Über den Tivoli-Desktop

Führen Sie folgende Schritte aus, um den Remote Control-Server über den Tivoli-Desktop zu installieren:

1. Wählen Sie nacheinander **Desktop → Installieren → Produkt installieren** aus, um den Dialog 'Produkt installieren' anzuzeigen.

   Sollte die Serverkomponente von Remote Control nicht unter **Zu installierendes Produkt auswählen** aufgelistet sein, fahren Sie mit Schritt 2 fort. Ist dies nicht der Fall, fahren Sie direkt mit Schritt 3 fort.
2. Klicken Sie auf **Datenträger auswählen**, um den Dialog 'Datei-Browser' aufzurufen.

   Über den Datei-Browser können Sie den Pfad des Installationsdatenträgers feststellen bzw. angeben.

- **Wenn Sie den Pfad des CD-ROM-Images kennen:**
  a. Geben Sie im Feld **Pfadname** den vollständigen Pfad ein.
  b. Klicken Sie auf **Pfad festlegen**, um in das angegebene Verzeichnis zu wechseln.
  c. Klicken Sie auf die Schaltfläche **Datenträger festlegen & Schließen**, um den neuen Datenträgerpfad zu speichern und zum Dialog 'Produkt installieren' zurückzukehren. Dieser Dialog enthält nun eine Liste der für die Installation verfügbaren Produkte.
- **Wenn Sie den Pfad des CD-ROM-Images nicht kennen:**
  a. Wählen Sie aus dem Listenfeld **Hosts** den Host aus, auf dem sich die Installationsimages befinden. Dadurch wird die Liste **Verzeichnisse** aktualisiert, so dass die Verzeichnisse des von Ihnen ausgewählten Hosts dort jetzt auch aufgelistet werden.
  b. Wählen Sie aus dem Listenfeld **Verzeichnisse** das Verzeichnis aus, in dem sich die Installationsimages befinden.
  c. Klicken Sie auf die Schaltfläche **Datenträger festlegen & Schließen**, um den neuen Pfad der Installationsimages zu speichern und zum Dialog 'Produkt installieren' zurückzukehren. Dieser Dialog enthält nun eine Liste der für die Installation verfügbaren Produkte.

3. Wählen Sie in der Liste **Zu installierendes Produkt auswählen** den Eintrag 'Tivoli Remote Control Server 3.8' aus.
4. Geben Sie mit Hilfe der Pfeiltasten die Clients an, auf denen die ausgewählte Komponente installiert werden soll. Mit diesen Tasten können Sie die Namen der Clients zwischen den Listen **Clients für die Installation** und **Verfügbare Clients** verschieben.

   Anmerkung: Eine Fehlernachricht wird angezeigt, falls eine Tivoli Remote Control-Komponente auf einem ungültigen Maschinentyp installiert wird.
5. Klicken Sie auf die Schaltfläche **Installieren**, um die Komponente zu installieren. Daraufhin wird der Dialog 'Produktinstallation' aufgerufen. Dort werden die Operationen aufgeführt, die während der Installation ausgeführt werden. Außerdem erhalten Sie in diesem Dialog Warnungen zu allen Problemen, die Sie möglicherweise vor der Installation der Komponente beheben sollten.
6. Klicken Sie auf **Installation fortsetzen**, um mit der Installation zu beginnen. Im Dialog 'Produktinstallation' werden während der Installation Statusinformationen angezeigt. Nach Abschluss der Installation zeigt der Dialog 'Produktinstallation' eine Abschlussnachricht an.
7. Klicken Sie auf **Schließen**, um zum Dialog 'Produkt installieren' zurückzukehren.

Geben Sie auf den Tivoli-Gateways, auf denen Sie den Remote Control-Server installiert haben, in der Eingabeaufforderung folgendes ein:

```
wgateway <Gatewaykennung> restart
```

Den Befehl 'winstall' verwenden

Mit dem Befehl im folgenden Beispiel wird die Serverkomponente von Remote Control auf einem verwalteten Knoten installiert. Führen Sie **winstall** aus.

```
winstall -c cdrom_Verz -s Produktserver -i Datei
@CreatePaths@=1 Knoten1 Knoten2
```

Schritt 1: Tivoli Remote Control-Server installieren

Dabei gilt:

-c *cdrom_Verz*	Gibt den Pfad des CD-ROM-Images an.
-s *Produktserver*	Gibt den Namen des verwalteten Knotens an, auf dem sich das CD-ROM-Image der Tivoli Remote Control-Anwendung befindet.
-i *Datei*	Gibt die indexierte Datei an, über die die Komponenten von Tivoli Remote Control installiert werden. Das Argument *Datei* steht für folgendes: **RC_ALI** Installiert die Serverkomponente von Remote Control auf dem Tivoli-Server oder anderen verwalteten Knoten im lokalen Bereich.
@CreatePaths@=1	Erstellt beliebiges Verzeichnis, falls dies noch nicht vorhanden ist.
Knoten1 Knoten2	Gibt die Namen der verwalteten Knoten an, auf denen der Server installiert werden soll, wenn TCP als Knotenprotokoll verwendet wird. Falls keine Angabe von Knoten erfolgt, wird die Komponente auf allen Knoten des aktuellen Bereichs installiert.

Weitere Informationen zu diesem Befehl erhalten Sie, wenn Sie in der Eingabeaufforderung **winstall** eingeben, oder entnehmen Sie dem Handbuch *Tivoli Management Framework Reference Guide*.

Geben Sie auf den Tivoli-Gateways, auf denen Sie den Remote Control-Server installiert haben, in der Eingabeaufforderung folgendes ein:

```
wgateway <Gatewaykennung> restart
```

Schritt 2: Controller und Ziele auf Endpunkten installieren

Die Software von Tivoli Remote Control muss nicht manuell auf den Endpunkten installiert werden. Wenn Sie eine Remote Control-Sitzung zum ersten Mal von einem Endpunkt aus starten, entweder über den Tivoli-Desktop oder mit dem Befehl **wrc** (wie unter „wrc" auf Seite 154 beschrieben) oder über die Webschnittstelle, wird die Controller-Software von Remote Control auf diesem Endpunkt installiert. Die Zielsoftware von Remote Control wird auf dem Endpunkt installiert, der vom Controller zum Starten einer Sitzung aufgefordert wird.

Nach Abschluss der Installation eines Remote Control-Ziels können Sie eine Remote Control-Sitzung im eingeschränkten Modus ausführen. Ein Neustart ist hierfür nicht erforderlich. Weitere Informationen finden Sie unter „Sitzung im eingeschränkten Modus" auf Seite 16. Wenn der Zielrechner neu gestartet wurde, können Sie eine Remote Control-Sitzung im vollständig funktionsfähigen Modus ausführen. OS/2-Controller und OS/2-Zielrechner müssen nach Abschluss der Installation immer neu gestartet werden.

Beim ersten Start einer Dateiübertragungs- oder Chat-Sitzung wird derselbe Installationsvorgang ausgeführt. Bevor eine Dateiübertragungs- oder Chat-Sitzung unter Windows NT, Windows XP oder Windows 2000 gestartet wird, prüft Tivoli Remote Control unter Verwendung des Konfigurationsmanagers von Tivoli, ob JRE 1.3 auf dem Controller und dem Zielrechner installiert ist. Ist dies nicht der Fall, haben Sie zwei Möglichkeiten: Installieren Sie vor Ausführung einer Dateiübertragungs- oder Chat-Sitzung JRE 1.3 mit dem Befehl **wrcinstep**, oder installieren Sie JRE 1.3 mit dem Befehl **wrc** bzw. über die Schnittstelle von Tivoli Remote Control, wenn Sie eine Dateiübertragungs- oder Chat-Sitzung zum ersten Mal star-

ten. Unter Umständen verzögert sich der Start der Sitzung um einige Minuten, wenn die Installation von JRE 1.3 erforderlich ist.

Wenn Sie Tivoli Remote Control oder JRE 1.3 in einer großen Umgebung auf mehreren Endpunkten gleichzeitig installieren müssen, verwenden Sie den Befehl **wrcinstep**, wie unter „wrcinstep" auf Seite 157 beschrieben.

Anmerkung: Wenn Sie in einem Bereich von Tivoli Management Framework Version 4.1 Tivoli Remote Control auf mehreren Endpunkten, die auf derselben Maschine ausgeführt werden, installieren möchten, müssen Sie sicherstellen, dass auf den Gateways, die diese Endpunkte verwalten, dieselbe Version von Tivoli Remote Control ausgeführt wird.

Den Treiber von IBM Tivoli Remote Control auf Windows XP-Zielrechnern installieren

Wenn Sie eine Sitzung auf einem Windows NT- oder Windows 2000-Zielrechner starten, installiert IBM Tivoli Remote Control 3.8 einen Spiegeltreiber im Kernelmodus. Dieser Treiber heißt IBM Tivoli Remote Control Driver. Er optimiert die Leistung, ist jedoch für die Durchführung von Remote Control-Operationen nicht zwingend notwendig. Beim Start einer Remote Control-Sitzung mit einer Windows XP-Zielmaschine, werden Sie dazu aufgefordert, die Installation des Treibers von IBM Tivoli Remote Control zu akzeptieren. Wenn Sie auf **OK** klicken, sollten Sie die aktuelle Sitzung schließen und eine neue Sitzung starten.

Sie können die Installation auch ablehnen, indem Sie auf **Ignorieren** klicken. Wenn die Sicherheitsbestimmungen auf Windows XP-Zielrechnern gelockert sind, wird der Treiber von IBM Tivoli Remote Control von Tivoli Remote Control automatisch installiert.

Sie haben folgende Möglichkeiten, um den Treiber von IBM Tivoli Remote Control auf Windows XP-Zielrechnern zu installieren:

- Sie können die Sicherheitsbestimmungen auf allen Windows XP-Zielrechnern lokal lockern.
- Sie können die Sicherheitsbestimmungen zentral lockern, indem Sie die Installationsrichtlinie des domänenübergreifenden Treibers konfigurieren (wenn die Windows XP-Zielrechner zu einer Active Directory-Domäne gehören).

Führen Sie einen der folgenden Vorgänge aus, um die Leistung zu verbessern:

- Befolgen Sie die Anweisungen im Artikel 298503 der Microsoft Knowledge Base, um die Installation des Treibers von Tivoli Remote Control lokal auszuführen:

  "Driver Signing Policy Values Cannot Be Modified Directly in Windows XP" (http://support.microsoft.com?kbid=298503).
- Führen Sie die Installation des Treibers von IBM Tivoli Remote Control Driver auf Domänenbasis aus:
  1. Befolgen Sie hierzu die Anweisungen im Artikel 298503 der Microsoft Knowledge Base:

     "Driver Signing Policy Values Cannot Be Modified Directly in Windows XP" (http://support.microsoft.com?kbid=298503).
  2. Befolgen Sie die Anweisungen im Artikel 324230 der Microsoft Knowledge Base:

     "A Domain Driver-Signing Policy Is Not Applied" (http://support.microsoft.com?kbid=324230).

3. Stellen Sie sicher, dass die Änderungen an der Treibersignierungs-Richtlinie auf allen Windows XP-Zielrechnern in der Active Directory-Domäne durchgeführt werden.

Sitzung im eingeschränkten Modus

Nach Abschluss der Installation eines Remote Control-Ziels auf einer Windows-Plattform können Sie eine Remote Control-Sitzung im eingeschränkten Modus ausführen. Ein Neustart ist hierfür nicht erforderlich.

Je nach Betriebssystem des Zielrechners gelten für die Sitzung folgende Einschränkungen:

Windows XP-, Windows 2000- und Windows NT-Zielrechner:

- Während einer aktiven Sitzung sind die Tastatur und die Maus nur dann gesperrt, wenn auf dem Zielrechner der Standarddesktop zum Einsatz kommt.
- Die DOS-Gesamtanzeige wird im Remote Control-Fenster nicht angezeigt.
- Unter Umständen kann keine optimale Leistung erzielt werden. Dies gilt nur für Windows NT-Zielrechner.

Zielrechner mit Windows 98 Second Edition:

- Die Tastatur und die Maus sind während einer aktiven Sitzung nicht gesperrt.
- Die DOS-Gesamtanzeige wird im Remote Control-Fenster nicht angezeigt.

Nachdem der Zielrechner neu gestartet wurde, können Sie eine Remote Control-Sitzung im vollständig funktionsfähigen Modus ausführen.

Integration mit der Datenbank für Tivoli Inventory

IBM Tivoli Inventory kann die Maschinen in Ihrer Tivoli Management Region (TMR) durchsuchen und Hardware- und Softwaredaten erfassen, die in einer Datenbank namens Konfigurationsrepository gespeichert werden. Die Zielinstallation erstellt die Signaturdatei *EQN380.SIG*. Mit Hilfe dieser Datei kann Tivoli Inventory die Installation der Ziele feststellen und das Konfigurationsrepository mit den Zielnamen automatisch aktualisieren.

Zum Abrufen der Liste mit den Zielworkstations müssen Sie einen der folgenden Schritte ausführen:

- Aktualisieren Sie die Konfigurationsdatei der Softwaresignatur 'SWSIGS.INI' manuell.
- Fügen Sie die Signatur von Tivoli Remote Control Version 38 hinzu, indem Sie den Befehl **winvsig** über die Befehlszeile von Inventory ausführen:

```
winvsig -a -d "Tivoli Remote Control" -n EQN380.SIG -s 6 -v 3.8
```

Weitere Informationen finden Sie im *Tivoli Inventory Benutzerhandbuch*.

Schritt 3: Das Tivoli Remote Control-Gateway auf verwalteten Knoten installieren

Um das Remote Control-Gateway auf einem verwalteten Knoten zu installieren, müssen Sie den Remote Control-Server installieren und die Richtlinienmethode 'rc_def_gw' wie auf Seite 79 beschrieben setzen.

Anmerkungen:

1. In früheren Releases von Tivoli Remote Control wurde anstelle des Remote Control-Proxys das Remote Control-Gateway für die Kommunikation über Firewalls verwendet. Wenn Sie den Port des Remote Control-Gateways mit Ihrer

Firewall-Konfiguration abgleichen, können alle Controller über dasselbe Remote Control-Gateway auf alle Ziele, die sich auf der anderen Seite der Firewall befinden, zugreifen.

2. Das Remote Control-Gateway kann nicht zur Überbrückung zweier verschiedener LAN-Segmente verwendet werden.
3. Auf einem verwalteten Knoten kann ein Gateway bis zu 32 eingehende Anschlüsse und bis zu 64 Sitzungen pro eingehenden Port verwalten.

Schritt 4: Den Tivoli Remote Control-Proxy installieren

Vor der Installation des Remote Control-Proxys müssen Sie sicherstellen, dass Sie über grundlegende Informationen zur Proxykonfiguration verfügen wie beispielsweise die Berechtigungsklasse des Proxys, Verbindungsart oder Portnummern.

Informationen zur Erfassung all dieser Daten und zur Installation des Remote Control-Proxys können Sie dem Kapitel 3, „Sitzungen über Firewalls ausführen", auf Seite 25 entnehmen.

Upgrades von früheren Releases

In diesem Abschnitt wird erläutert, wie Sie ein Upgrade von Version 3.7.1 auf Tivoli Remote Control Version 3.8 ausführen. Informationen zur Durchführung von Upgrades für frühere Releases als 3.7.1 finden Sie in den *Release-Notes für Tivoli Remote Control Version 3.7.1*.

Sie können folgende Upgrades durchführen:

- Für einzelne Bereiche. Siehe „Upgrade einer einzelnen Tivoli Management Region (TMR)" auf Seite 17.
- Für verbundene Bereiche. Siehe „Upgrade für verbundene Bereiche ausführen" auf Seite 22.

Upgrade einer einzelnen Tivoli Management Region (TMR)

Sie können folgende Upgrades für den Bereich durchführen:

- Ein Upgrade des Tivoli-Servers und aller Gateways auf Tivoli Remote Control Version 3.8 (vollständiger Upgrade).
- Ein Upgrade des Tivoli-Servers und eines oder mehrerer Gateways auf Tivoli Remote Control Version 3.8 (Teil-Upgrade). In diesem Fall müssen Sie die Implementierung des Bereichs planen, indem Sie festlegen, für welches Gateway zum jetzigen Zeitpunkt und für welches Gateway zu einem späteren Zeitpunkt ein Upgrade ausgeführt werden soll.

  Anmerkung: Wenn Sie einen Endpunkt mit einer alten Version von Tivoli Remote Control benötigen, müssen Sie das Richtlinienscript 'select_gateway_policy' für den Endpunkt konfigurieren, um die Gruppe der Gateways für die Verwaltung dieses Endpunkts festzulegen. Für diese Gateways darf kein Upgrade ausgeführt werden.

Ein Upgrade für einen Bereich von Version 3.7.1 auf Version 3.8 ausführen

In diesem Szenario gehört ein Server von Remote Control Version 3.7.1, der auf einem Tivoli-Server und auf allen Gateways des Bereichs installiert ist, zur Kernumgebung. Auf allen verwalteten Endpunkten wird Tivoli Remote Control Version 3.7.1 ausgeführt.

Upgrade einer einzelnen Tivoli Management Region (TMR)

Anmerkung: Durch den Upgrade auf Tivoli Remote Control Version 3.8 ändert sich die Syntax einiger Richtlinienmethoden. Die Standardwerte für die Richtlinienmethoden werden von den alten Richtlinienmethoden übernommen. Im Verzeichnis '%DBDIR%' befinden sich Sicherheitskopien der folgenden alten Richtlinienmethoden: rc_def_ports, rc_def_define, rc_def_gw, rc_def_unchekedlist und rc_def_commands:

- def_ports_*RemoteControl_default_policy_object_name*.bk
- def_define_*RemoteControl_default_policy_object_name*.bk
- def_gw_*RemoteControl_default_policy_object_name*.bk
- def_uncheckedlist_*RemoteControl_default_object_policy_name*.bk
- def_cmd_*RemoteControl_default_object_policy_name*.bk

Vollständiger Upgrade: Führen Sie folgende Schritte aus, um für den Bereich einen Upgrade auszuführen:

1. Installieren Sie Tivoli Remote Control Server 3.8 Upgrade auf dem Tivoli-Server und allen Gateways wie unter „Upgrade-Methoden" auf Seite 20 beschrieben.
2. Führen Sie auf den Tivoli-Gateways, auf denen Sie den Remote Control-Server installiert haben, folgenden Befehl aus:

   ```
   wgateway <Gatewaykennung> restart
   ```

3. Installieren Sie Tivoli Remote Control Version 3.8 auf dem Controller und den Zielendpunkten. Führen Sie hierzu einen der folgenden Schritte aus:
   - Führen Sie den Befehl **wrcinstep** aus. Weitere Informationen zum Befehl **wrcinstep** finden Sie unter „wrcinstep" auf Seite 157.
   - Starten Sie eine Tivoli Remote Control-Sitzung. Tivoli Remote Control Version 3.8 wird von den Gateways, die die Endpunkte verwalten, automatisch heruntergeladen.
4. Unter OS/2 müssen Sie die Controller-Workstations neu starten, wenn Sie dazu aufgefordert werden. Wenn Sie für Ziele, die auf anderen Plattformen installiert sind, keinen Neustart durchführen, wird die Sitzung im eingeschränkten Modus ausgeführt. Weitere Informationen hierzu finden Sie unter „Sitzung im eingeschränkten Modus" auf Seite 16.
5. Unter Windows 2000 und Windows XP müssen Sie auf den Zielworkstations einen Neustart durchführen, um alle Funktionen von Tivoli Remote Control Version 3.8 nutzen zu können.

Teil-Upgrade: Mit den folgenden Schritten können Sie einen Teil-Upgrade für einen Bereich ausführen. Auf diese Weise können Sie die Arbeit mit Ziel- und Controller-Endpunkten, auf denen Tivoli Remote Control Version 3.7.1 ausgeführt wird, fortsetzen.

Führen Sie folgende Schritte aus, um für den Bereich einen Upgrade auszuführen:

1. *Es ist wichtig, dass Sie den ersten Schritt korrekt ausführen.* Aus Kompatibilitätsgründen müssen Sie das Tivoli Remote Control Fixpack 01 - PTF U484604 (3.7.1-RCL-FP01) oder höher auf dem Tivoli-Server und auf den Gateways, auf denen Tivoli Remote Control Version 3.7.1 weiterhin ausgeführt wird, installieren, wenn die Version 3.8 auf dem Tivoli-Server installiert wird. Sie müssen dieses Fixpack installieren, bevor Sie für die anderen Gateways einen Upgrade auf Tivoli Remote Control Version 3.8 ausführen.
2. Installieren Sie Tivoli Remote Control Server 3.8 Upgrade auf dem Tivoli-Server und auf allen Gateways, die Sie auf Version 3.8 aktualisieren möchten (siehe „Upgrade-Methoden" auf Seite 20).

3. Führen Sie auf den Tivoli-Gateways, auf denen Sie den Remote Control-Server installiert haben, folgenden Befehl aus:

   ```
   wgateway <Gatewaykennung> restart
   ```

4. Führen Sie einen der folgenden Schritte aus, um Tivoli Remote Control Version 3.8 auf den Controller- und Zielendpunkten, die von den aktualisierten Gateways gesteuert werden, zu installieren:
   - Führen Sie den Befehl **wrcinstep** aus. Weitere Informationen zum Befehl **wrcinstep** finden Sie unter „wrcinstep" auf Seite 157.
   - Starten Sie eine Tivoli Remote Control-Sitzung. Tivoli Remote Control Version 3.8 wird von den Gateways, die die Endpunkte verwalten, automatisch heruntergeladen.
5. Unter OS/2 müssen Sie die Controller-Workstations neu starten, wenn Sie dazu aufgefordert werden. Wenn Sie für Ziele, die auf anderen Plattformen ausgeführt werden, keinen Neustart durchführen, wird die Sitzung im eingeschränkten Modus ausgeführt. Weitere Informationen hierzu finden Sie unter „Sitzung im eingeschränkten Modus" auf Seite 16.
6. Unter Windows 2000 und Windows XP müssen Sie die Zielworkstations neu starten, um alle Funktionen von Tivoli Remote Control Version 3.8 nutzen zu können.

Nach dem Teil-Upgrade Ihres Bereichs auf Tivoli Remote Control Version 3.8 und vor dem Start einer Sitzung sollten Sie Folgendes beachten:

- Wenn Sie einen Endpunkt zu einem Bereich hinzufügen und der Endpunkt nicht über die Binärdateien des Controllers und des Zielrechners verfügt, müssen Sie sicherstellen, dass der Endpunkt von einem Gateway mit Tivoli Remote Control Version 3.8 verwaltet wird.
- Stellen Sie sicher, dass Sie lediglich ein Tool von Tivoli Remote Control Version 3.8 verwenden.
- Controller mit Tivoli Remote Control Version 3.8 können Remote Control-Sitzungen mit Zielrechnern mit Tivoli Remote Control Version 3.8 oder Fixpack 01 starten.
- Dateiübertragungs-Controller mit Tivoli Remote Control Version 3.8 können keine Sitzungen mit Zielrechnern mit Fixpack 01 starten.
- Dateiübertragungs- und Chat-Controller mit Fixpack 01 können Sitzungen mit Zielrechnern mit Fixpack 01 starten.
- Für Sitzungen zwischen Endpunkten mit Fixpack 01 sind die Richtlinienmethoden 'rc_def_encryption', 'rc_def_proxy' und 'rc_def_optimize' nicht gültig.
- Die Version des Controllers muss mit der des Zielrechners übereinstimmen oder höher sein (Beispiel: Wenn auf dem Zielrechner Version 3.7.1 ausgeführt wird, muss auf dem Controller Version 3.7.1 oder 3.8 ausgeführt werden).

In den folgenden Tabellen sind die Aktionen aufgeführt, die in Umgebungen unterstützt werden, in denen sowohl Tivoli Remote Control Version 3.7.1 mit Fixpack 01 (wird in der Tabelle als Fixpack 01 bezeichnet) und Tivoli Remote Control Version 3.8 (wird in der Tabelle als 3.8 bezeichnet) zum Einsatz kommen.

- Remote Control-Aktionen und Neustart.

Tivoli-Server	Remote Control-Tool	Controller	Ziel	Unterstützt
Fixpack 01	Fixpack 01	Fixpack 01	Fixpack 01	Ja
3.8	Fixpack 01	Fixpack 01	Fixpack 01	Nein

Upgrade einer einzelnen Tivoli Management Region (TMR)

Tivoli-Server	Remote Control-Tool	Controller	Ziel	Unterstützt
3.8	3.8	Fixpack 01	Fixpack 01	Ja
3.8	3.8	3.8	Fixpack 01	Ja
3.8	3.8	3.8	3.8	Ja

- Dateiübertragungs- und Chat-Aktionen.

Tivoli-Server	Remote Control-Tool	Controller	Ziel	Unterstützt
Fixpack 01	Fixpack 01	Fixpack 01	Fixpack 01	Ja
3.8	Fixpack 01	Fixpack 01	Fixpack 01	Nein
3.8	3.8	Fixpack 01	Fixpack 01	Ja
3.8	3.8	3.8	Fixpack 01	Nur Chat
3.8	3.8	3.8	3.8	Ja

Upgrade-Methoden

Für den Upgrade der Komponenten Tivoli-Server und verwalteter Knoten von Tivoli Remote Control Version 3.7.1 auf Tivoli Remote Control Version 3.8 können Sie eine der folgenden Methoden anwenden:

- Mit dem Tivoli Software Installation Service (SIS). Weitere Informationen hierzu finden Sie im Handbuch *Tivoli Software Installation Service User's Guide*.
- Über den Tivoli-Desktop.
- Mit dem Befehl **wpatch** von Tivoli Management Framework.

Bevor Sie den Upgrade auf Tivoli Remote Control Version 3.8 unter Anwendung einer der oben genannten Methoden ausführen, müssen Sie sicherstellen, dass Sie

- den Fixpack 01 installiert haben.
- über die Berechtigungsklasse 'super' oder 'install-product' verfügen.

Tivoli Software Installation Service (SIS) verwenden: Vor der Installation des Remote Control-Servers unter Verwendung von SIS müssen Sie sicherstellen, dass Sie die Programmkorrekturen '3.7-SIS-DEPOT-0005' und '3.7-SISCLNT-0005' ausgeführt haben.

Gehen Sie wie folgt vor, um für die Komponenten von Tivoli Remote Control unter Verwendung von SIS einen Upgrade auszuführen:

1. Importieren Sie die Produktimages in das SIS-Depot.
2. Wählen Sie die zu installierenden Komponenten aus.
3. Wählen Sie die Maschinen aus, auf denen die jeweiligen Komponenten installiert werden sollen.
4. Klicken Sie auf **Installieren**.

Weitere Informationen zur Verwendung des Tivoli Software Installation Service für den Upgrade von Komponenten finden Sie im Handbuch *Tivoli Enterprise Console Benutzerhandbuch*.

Tivoli-Desktop verwenden: Wenn Tivoli Remote Control Version 3.7.1 auf Ihren Maschinen installiert ist und Sie einen Upgrade auf Tivoli Remote Control Version 3.8 ausführen möchten, führen Sie folgende Schritte aus:

Upgrade einer einzelnen Tivoli Management Region (TMR)

1. Wählen Sie im Menü **Desktop** die Optionen **Installieren→ Programmkorrektur installieren** aus, um den Dialog 'Programmkorrektur installieren' anzuzeigen.
2. Sollten die Tivoli Remote Control-Komponenten nicht in der Liste **Zu installierende Programmkorrektur auswählen**, enthalten sein, klicken Sie auf **Datenträger auswählen**, um den Pfad zum Installationsdatenträger anzugeben.
3. Wählen Sie aus dem Listenfeld **Zu installierende Programmkorrektur auswählen** den Eintrag **Tivoli Remote Control Server Upgrade 3.8** aus. Mit dieser Komponente wird der Remote Control-Server auf dem Tivoli-Server oder anderen verwalteten Knoten in der lokalen Tivoli Management Region (TMR) aktualisiert.
4. Verwenden Sie die Pfeiltasten, um die Clients anzugeben, auf denen für die ausgewählte Komponente ein Upgrade ausgeführt werden soll. Mit diesen Tasten können Sie die Namen der Clients zwischen den Listen **Clients für die Installation** und **Verfügbare Clients** verschieben.
5. Klicken Sie auf **Installieren**, um die Komponentenerweiterung zu starten. Im Dialog 'Installation der Programmkorrektur' werden die Operationen aufgeführt, die während der Installation ausgeführt werden. Außerdem erhalten Sie in diesem Dialog Warnungen zu allen Problemen, die Sie möglicherweise vor Installation der Komponentenerweiterung beheben sollten.
6. Klicken Sie auf **Installation fortsetzen**, um mit der Installation zu beginnen. Im Dialog 'Installation der Programmkorrektur' wird der Status während der Installation angezeigt.

   Nach Abschluss der Installation wird im Dialog 'Installation der Programmkorrektur' eine Abschlussnachricht angezeigt.
7. Klicken Sie auf **Schließen**, um zum Dialog 'Installation der Programmkorrektur' zurückzukehren.

Den Befehl 'wpatch' verwenden: Im Folgenden werden Beispiele zur Verwendung des Befehls **wpatch** für die Ausführung eines Upgrades von Tivoli Remote Control aufgeführt.

Um die Serverkomponente von Remote Control auf dem Tivoli-Server 'jupiter' über ein CD-ROM-Image zu installieren, führen Sie folgenden Befehl aus:

```
wpatch -c \root\images\upgrade -i RCALI38U.IND jupiter
```

Dabei gilt:

-c \root\images\upgrade	Gibt den Pfad des CD-ROM-Images an.
-i RCALI38U.IND	Gibt die indexierte Datei für die Produktinstallation an, in der die Programmkorrektur installiert wird.
jupiter	Gibt den verwalteten Knoten an, auf dem die Programmkorrektur installiert wird.

Anmerkung: Wenn Sie keinen verwalteten Knoten angeben, wird die Programmkorrektur auf allen verwalteten Knoten in der Tivoli Management Region (TMR) installiert, auf denen das Basisprodukt momentan installiert ist.

Weitere Informationen zum Befehl **wpatch** finden Sie im Handbuch *Tivoli Management Framework Reference Guide*.

Upgrade für verbundene Bereiche ausführen

Je nach Bedarf können Sie für jeden Bereich einen vollständigen Upgrade oder einen Teil-Upgrade ausführen. Führen Sie für alle Bereiche die unter „Upgrade einer einzelnen Tivoli Management Region (TMR)" auf Seite 17 beschriebenen Schritte aus.

Unterschiedliche Versionen in verbundenen Bereichen verwenden

Beim Starten von Sitzungen zwischen Controllern und Zielen, die verbundenen Bereichen angehören, von denen für einen Bereich ein Upgrade auf Tivoli Remote Control Version 3.8 ausgeführt wurde, muss Folgendes beachtet werden:

- Controller, die zu aktualisierten Bereichen gehören, müssen zum Starten von Remote Control-Sitzungen mit Zielen, die zu nicht aktualisierten Bereichen gehören, ein Tool von Tivoli Remote Control Version 3.8 verwenden.
- Controller, die zu aktualisierten Bereichen gehören, können keine Sitzungen zur Dateiübertragung mit Zielen starten, die zu nicht aktualisierten Bereichen gehören.
- Die Version des Controllers muss mit der des Remote Control-Tools, das zum Starten einer Sitzung verwendet wird, übereinstimmen oder niedriger sein.
- Der Remote Control-Server, der zum Starten einer Sitzung verwendet wird, muss zur Tivoli Management Region (TMR) des Controllers gehören.

Tivoli Remote Control deinstallieren

Um Tivoli Remote Control zu deinstallieren, müssen Sie die Server, Proxys, Controller und Ziele von Tivoli Remote Control wie in den folgenden Abschnitten beschrieben entfernen:

- „Den Controller oder das Ziel deinstallieren"
- „Den Tivoli Remote Control-Server deinstallieren"
- „Den Tivoli Remote Control-Proxy deinstallieren" auf Seite 23

Den Controller oder das Ziel deinstallieren

Um den Controller oder das Ziel zu deinstallieren, verwenden Sie den Befehl **wrcuninstep** und starten Sie anschließend die Workstation neu. Informationen zu dem Befehl finden Sie unter „wrcuninstep" auf Seite 161.

Den Tivoli Remote Control-Server deinstallieren

Tivoli Management Framework stellt den Befehl **wuninst** zur Verfügung, mit dem Sie Tivoli-Anwendungen auf einem bestimmten verwalteten Knoten oder in der gesamten Tivoli Management Region (TMR) deinstallieren können. Bei dem Befehl **wuninst** handelt es sich um ein bestimmtes Script (Wrapper Script), mit dem produktspezifische Deinstallationsscripts aufgerufen werden.

Weitere Informationen zum Befehl **wuninst** finden Sie im Handbuch *Tivoli Management Framework Reference Manual*.

Tivoli Remote Control-Server deinstallieren

Der Remote Control-Server kann von jedem verwalteten Knoten in Ihrer Umgebung oder von der Tivoli Management Region (TMR) deinstalliert werden. Führen Sie hierzu folgende Schritte aus:

1. Schließen Sie alle Dialoge des Remote Control-Tools, das auf dem verwalteten Knoten ausgeführt wird.
2. Führen Sie den Befehl **wuninst** wie folgt aus. (Unter Windows 2000 müssen Sie den Befehl **wuninst** über eine Bash-Shell ausführen.)

   ```
   wuninst Komp_Kennung Knotenname [–rmfiles][-all]
   ```

   Dabei gilt:

   Komp_Kennung
   Gibt die Kennung der Tivoli Remote Control-Komponente an, die Sie deinstallieren möchten. Sie muss wie folgt lauten:

   RC_ALI Deinstalliert den Remote Control-Server.

   Knotenname Gibt den Knoten an, auf dem die Komponente deinstalliert wird. Wenn mit *Knotenname* der Tivoli-Server bezeichnet wird und die Option **-all** angegeben ist, wird die Anwendung aus der gesamten Tivoli Management Region (TMR) entfernt. Ihnen wird eine Bestätigungsnachricht angezeigt, bevor die Anwendung aus der Tivoli Management Region (TMR) entfernt wird.

   –rmfiles Gibt an, dass alle zugeordneten Dateien entfernt werden, unabhängig davon, ob es sich dabei um gemeinsam benutzte Dateien handelt.

   -all Wenn diese Option angegeben ist und mit *Knotenname* der Tivoli-Server bezeichnet wird, wird die Anwendung aus der gesamten Tivoli Management Region (TMR) entfernt.

   Standardmäßig werden ohne die Option**–rmfiles** nur die Datenbankeinträge für den angegebenen Knoten entfernt. Handelt es sich bei dem Knoten um den Tivoli-Server, werden mit dieser Option alle Datenbankobjekte entfernt.

Den Tivoli Remote Control-Proxy deinstallieren

Führen Sie zur Deinstallation der Remote Control-Proxys folgende Schritte aus:

- Unter Windows:
  1. Wählen Sie nacheinander **Start → Einstellungen → Systemsteuerung** aus.
  2. Doppelklicken Sie auf das Symbol **Software**.
  3. Wählen Sie 'IBM Tivoli Remote Control Proxy' aus.
  4. Klicken Sie auf **Hinzufügen/Entfernen**.
- Unter UNIX müssen Sie die Datei 'uninstall.sh' in folgendem Verzeichnis ausführen: *<Installationspfad für Remote Control-Proxy>*/_uninst

Tivoli Remote Control-Proxy deinstallieren

Kapitel 3. Sitzungen über Firewalls ausführen

Dieses Kapitel beschreibt, wie Tivoli Remote Control-Proxys installiert und konfiguriert werden müssen, um die Funktion von Tivoli Remote Control in einer Netzwerkumgebung mit einer oder mehreren Firewalls zu gewährleisten.

Bei diesem Umgebungstyp werden die Übertragungskanäle von der Firewall beschränkt. Mit Hilfe von verbundenen Remote Control-Proxys können Controller und Zielrechner unter Berücksichtigung der geltenden Firewallbestimmungen miteinander kommunizieren. Ein Remote Control-Proxy ist als *Controller-Proxy* mit dem Zielrechner verbunden. Der andere Remote Control-Proxy ist als *Zielproxy* mit dem Controller verbunden. Diese Proxys kommunizieren miteinander über die Firewall.

Einführung

Um die Remote Control-Proxys installieren bzw. deren Basiskonfiguration definieren zu können, müssen Sie zunächst folgende Vorgänge ausführen:

1. Die Firewalls und die Firewallbestimmungen, die für Ihre Umgebung gelten, identifizieren.
2. Die Position der Controller und Zielrechner in Bezug auf das Tivoli-Management-Gateway und die Firewalls definieren.
3. Feststellen, welche(s) Szenario(s), die unter „Identifikation Ihrer Szenarios" beschrieben werden, Ihrer Umgebung entsprechen.
4. Die Position der Komponenten von Tivoli Firewall Security Toolbox feststellen, wenn das Tivoli-Management-Gateway und die zugehörigen Endpunkte durch eine Firewall voneinander getrennt sind.
5. Festlegen, welcher Remote Control-Proxy dem anderen Proxy unter- bzw. übergeordnet ist. Siehe „Den Remote Control-Proxy als übergeordnetes oder untergeordnetes Element definieren" auf Seite 31.
6. Bei Verwendung der Komponenten von Tivoli Firewall Security Toolbox den Port des Zielproxys definieren bzw. bei Verwendung des Proxys im Standalone-Modus den Hostnamen und den Port des Zielproxys definieren. Siehe „Richtlinienmethode 'rc_def_proxy' für den Zielproxy konfigurieren" auf Seite 33.

Identifikation Ihrer Szenarios

Die Firewall-Szenarios, die von Tivoli Remote Control unterstützt werden, lassen sich je nach Position der Firewall in folgende Kategorien unterteilen: Bei allen Szenarios können mehrere Firewalls eingesetzt werden.

- Szenarios, in denen sich die Firewall zwischen dem Tivoli-Management-Gateway und dem Endpunkt befindet. In diesem Szenario müssen Sie die Remote Control-Proxys zusammen mit den Komponenten von Firewall Security Toolbox verwenden. Weitere Informationen finden Sie unter „Szenarios, die auf Firewall Security Toolbox basieren" auf Seite 26.

  Anmerkung: Die Remote Control-Proxys werden auch dann bei der Ausführung einer Sitzung zwischen einem Controller und einem Zielrechner verwendet, wenn sich deren Tivoli-Management-Gateway auf der anderen Seite der Firewall befindet.

- Szenarios, in denen verbundene Bereiche durch eine Firewall voneinander getrennt sind. In diesem Szenario werden ausschließlich die Remote Control-Proxys verwendet. Weitere Informationen finden Sie unter „Szenario mit dem Remote Control-Proxy im Standalone-Modus" auf Seite 31.

In diesen Szenarios wird NAT nur dann von Tivoli Remote Control unterstützt, wenn NAT den Remote Control-Proxys im privaten und öffentlichen Netzwerk permanente, statische Adressen zuweist.

Szenarios, die auf Firewall Security Toolbox basieren

In diesen Szenarios verwenden Sie den Remote Control-Proxy zusammen mit Firewall Security Toolbox, da nicht nur der Controller und der Zielrechner durch Firewalls voneinander getrennt werden, sondern auch das Tivoli-Management-Gateway und der zugehörige Controller- bzw. Zielendpunkt.

Der Remote Control-Proxy verwendet die Topologiedaten von Firewall Security Toolbox, die vom Endpunktproxy und vom Gateway-Proxy gespeichert werden, um eine geeignete Route zum Aufbau einer Verbindung zwischen dem Controller und dem Zielrechner über eine Reihe von Proxys zu suchen.

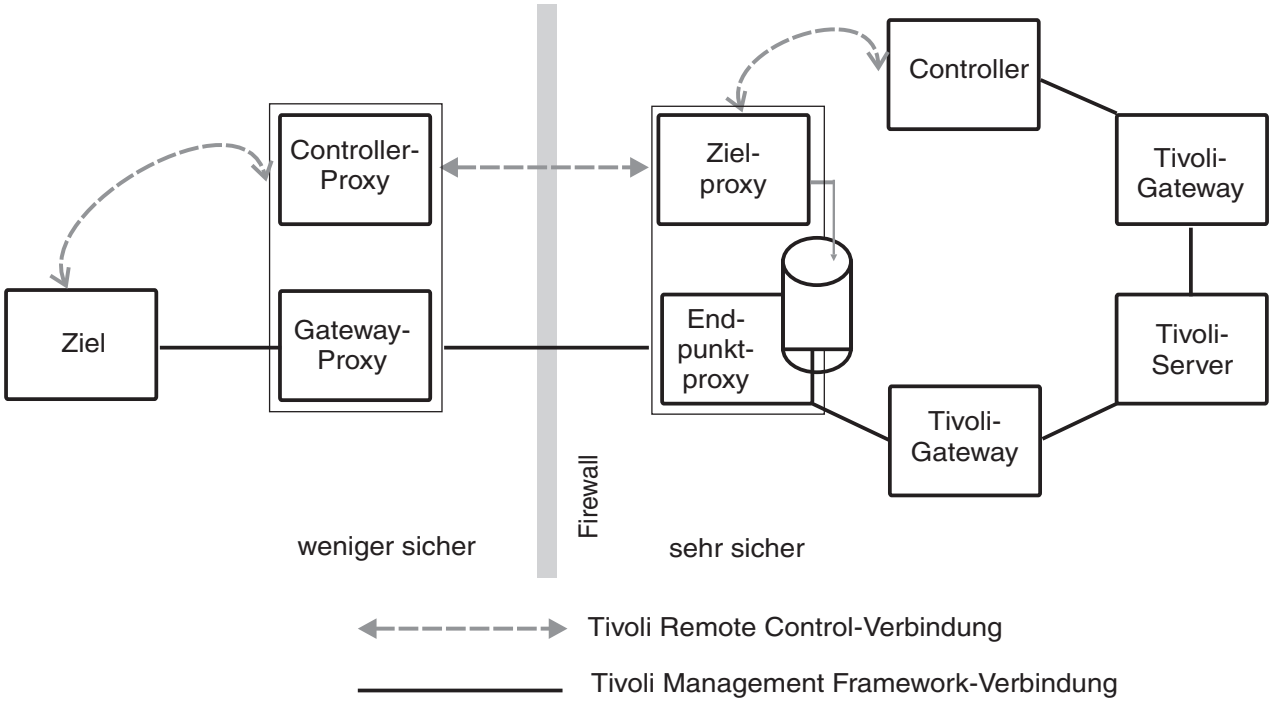
In diesen Szenarios müssen die Remote Control-Proxys auf derselben Maschine installiert werden, auf der auch der Endpunktproxy und der Gateway-Proxy ausgeführt werden. Darüber hinaus müssen die Kennungen des Gateway-Proxys und des Remote Control-Proxys, der auf der Workstation mit dem Gateway-Proxy installiert ist, identisch sein.

Anmerkung: Wenn es sich bei dem Endpunkt, auf dem Sie die Sitzung starten, ebenfalls um ein Remote Control-Proxy und ein Endpunktproxy handelt, müssen Sie den Befehl **wrc** verwenden. Informationen zu dem Befehl finden Sie unter „wrc" auf Seite 154.

In Netzwerken mit mehreren Firewalls, in denen zudem Endpunktproxys und Gateway-Proxys verwendet werden, müssen Sie eine weitere Komponente von Firewall Security Toolbox, das Relay, installieren. Siehe „Verwendung von mehreren Relays" auf Seite 30.

Controller auf der geschützten Seite

In diesem Szenario befindet sich der Controller auf der sicheren Seite der Firewall und das Ziel auf der weniger sicheren Seite.



Der Controller fordert den Start einer Sitzung mit einem Ziel an, das vom zugehörigen Tivoli-Management-Gateway durch eine Firewall getrennt ist. Die Anforderung (sie enthält die Netzwerkadressen des Controllers und des Ziels) wird an den Zielproxy weitergeleitet, der auf dem Endpunktproxyrechner ausgeführt wird.

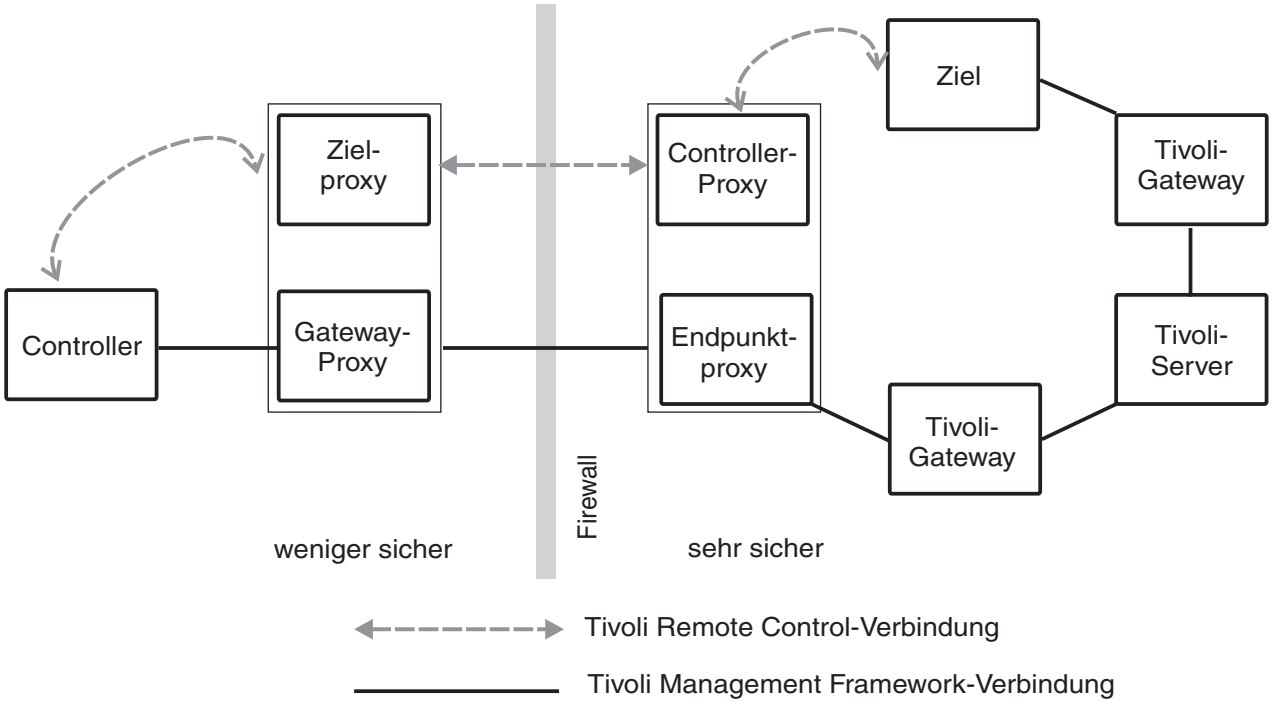
Der Zielproxy ermittelt die Kennung des Gateway-Proxys und die Adresse, unter der das Ziel im Gateway-Proxy registriert ist, indem er auf die Datenbank des Endpunktproxys zugreift. Anschließend übergibt der Zielproxy die Anforderung an den Controller-Proxy, der auf dem Gateway-Proxyrechner ausgeführt wird.

Anmerkung: Die Methode zum Herstellen einer Verbindung mit der Zielmaschine basiert auf der Tatsache, dass die Kennungen des Gateway-Proxys und des Remote Control-Proxys, die auf der Workstation mit dem Gateway-Proxy installiert sind, identisch sind.

Der Controller-Proxy startet die Sitzung mit dem in der Anforderung angegebenen Ziel.

Controller auf der ungeschützten Seite

In diesem Szenario befindet sich der Controller auf der ungeschützten Seite einer Firewall und das Ziel auf der sicheren Seite.

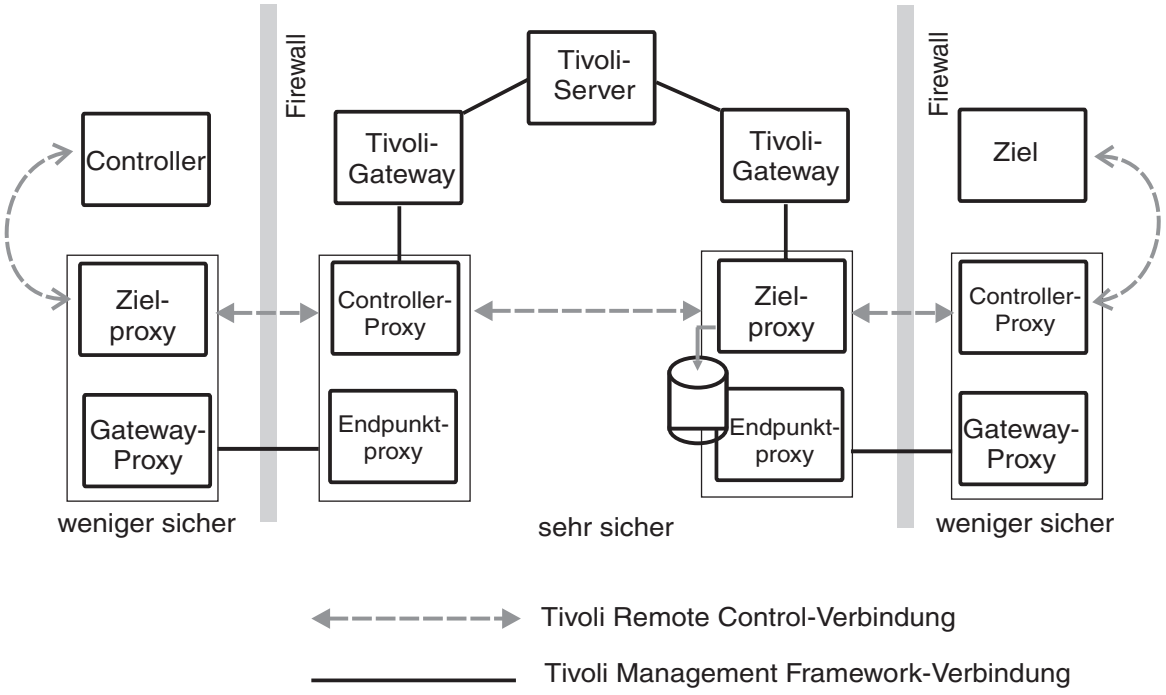


Der Controller, der vom zugehörigen Tivoli-Management-Gateway durch eine Firewall getrennt ist, fordert den Start einer Sitzung mit einem Ziel an.

Die Anforderung mit den Netzwerkadressen des Controllers und des Ziels wird an den Zielproxy weitergeleitet, der auf dem Gateway-Proxyrechner ausgeführt wird. Der Zielproxy übergibt die Anforderung an den Controller-Proxy, der auf dem Endpunktproxy ausgeführt wird. Daraufhin startet der Controller-Proxy die Sitzung mit dem in der Anforderung angegebenen Ziel.

Controller und Ziel außerhalb von Firewalls

In diesem Szenario sind der Controller und das Ziel unterschiedlichen Tivoli-Management-Gateways zugeordnet. Jedes Tivoli-Management-Gateway wird von den jeweiligen Endpunkten durch eine Firewall getrennt.

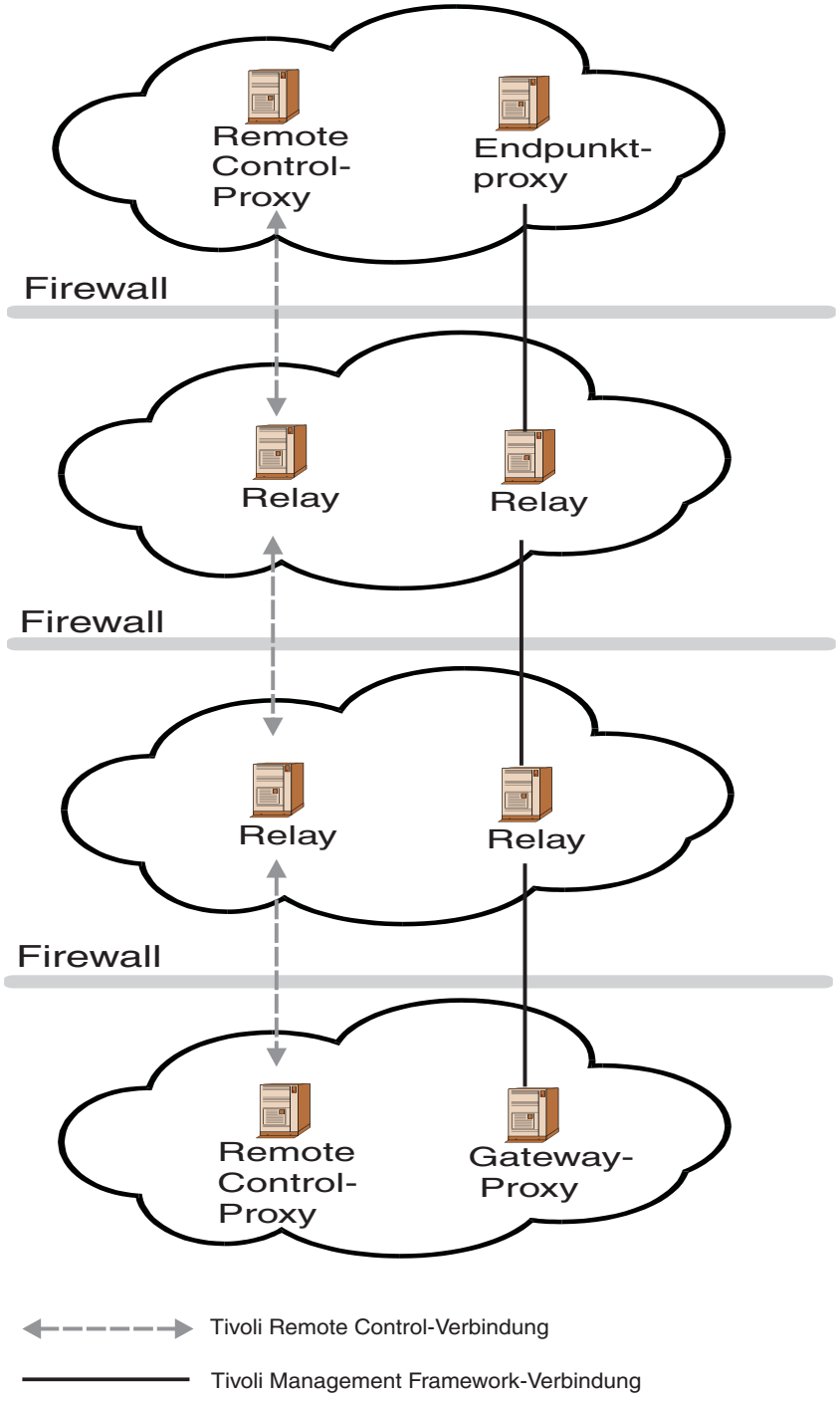


Der Controller fordert den Start einer Sitzung mit dem Ziel an. Die Anforderung (sie enthält die Netzwerkadressen des Controllers und des Ziels) wird an den Zielproxy weitergeleitet, der auf dem Gateway-Proxyrechner ausgeführt wird. Der Zielproxy übergibt die Anforderung an den Controller-Proxy, der auf dem Endpunktproxy ausgeführt wird.

Der Controller-Proxy kommuniziert mit dem Zielproxy, der auf dem Endpunktproxyrechner ausgeführt wird. Der Zielproxy identifiziert die Kennung des Gateway-Proxys und die Adresse, unter der das Ziel im Gateway-Proxy registriert ist, indem er auf die Datenbank des Endpunktproxys zugreift. Anschließend übergibt der Zielproxy die Anforderung an den Controller-Proxy, der auf dem Gateway-Proxyrechner ausgeführt wird. Der Controller-Proxy startet die Sitzung mit dem in der Anforderung angegebenen Ziel.

Verwendung von mehreren Relays

In all den zuvor beschriebenen Szenarios können Sie ein oder mehrere Relays für die Kommunikation über mehrere Firewalls verwenden (siehe Abbildung unten):



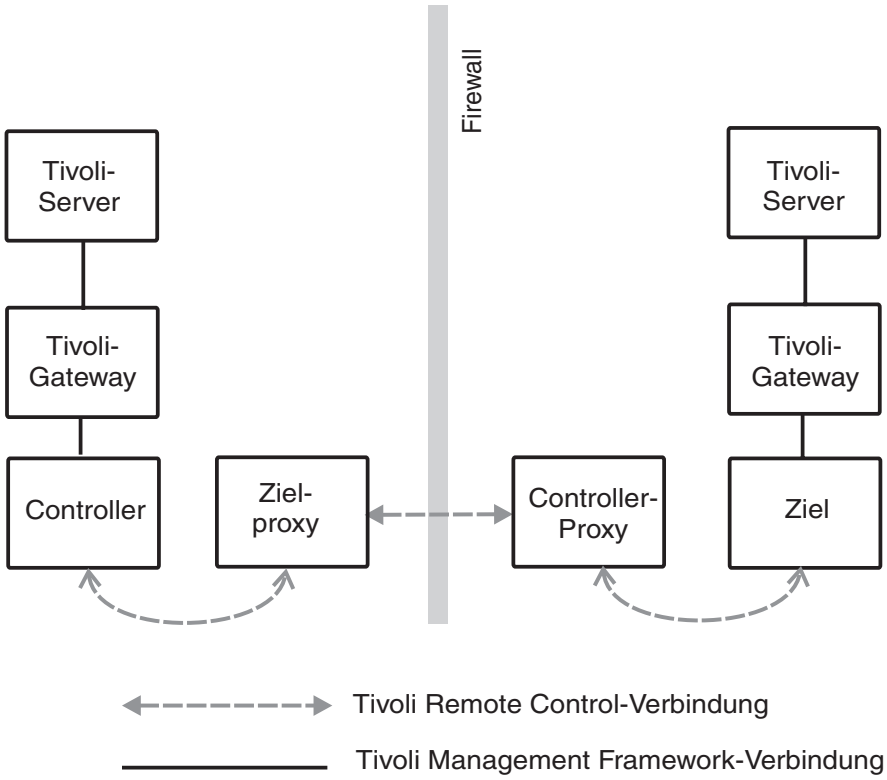
Bei Verwendung von Tivoli Firewall Security Toolbox zur Kommunikation über Firewalls müssen Sie sicherstellen, dass auf allen Relay-Rechnern zwei Relay-Instanzen installiert sind. Eine Instanz ist für die Kommunikation mit dem Endpunktproxy und dem Gateway-Proxy erforderlich, die andere Instanz wird für die Kommunikation mit den Remote Control-Proxys benötigt.

Szenario mit dem Remote Control-Proxy im Standalone-Modus

In diesem Szenario befinden sich das Tivoli-Management-Gateway und die zugehörigen Endpunkte auf derselben Seite der Firewall. Die Remote Control-Proxys können auf jeder beliebigen Maschine ausgeführt werden. Im Folgenden ist ein typisches Beispiel aufgeführt.

Ziel und Controller, die zu verbundenen Bereichen gehören, sind durch eine Firewall voneinander getrennt

In diesem Szenario gehören das Ziel und der Controller zu verbundenen Bereichen.



Der Controller stellt eine Verbindung zu dem in der Richtlinienmethode 'rc_def_proxy' angegebenen Zielproxy her. (Weitere Informationen finden Sie unter „Richtlinienmethode 'rc_def_proxy' für den Zielproxy konfigurieren" auf Seite 33.) Der Zielproxy stellt eine Verbindung zu dem in der Datei 'rcproxy.route' definierten Controller-Proxy her (weitere Informationen finden Sie unter „Den Pfad für untergeordnete Proxys in Szenarios mit dem Remote Control-Proxy im Standalone-Modus definieren" auf Seite 58) und sendet die Anforderung zum Herstellen einer Verbindung mit dem Zielrechner. Der Controller-Proxy verwendet die in der ersten Anforderung gespeicherten Zieldaten, um eine Sitzung mit dem Ziel zu starten.

Den Remote Control-Proxy als übergeordnetes oder untergeordnetes Element definieren

Vor der Konfiguration eines Remote Control-Proxys müssen Sie diesen als übergeordneten Remote Control-Proxy oder untergeordneten Remote Control-Proxy definieren.

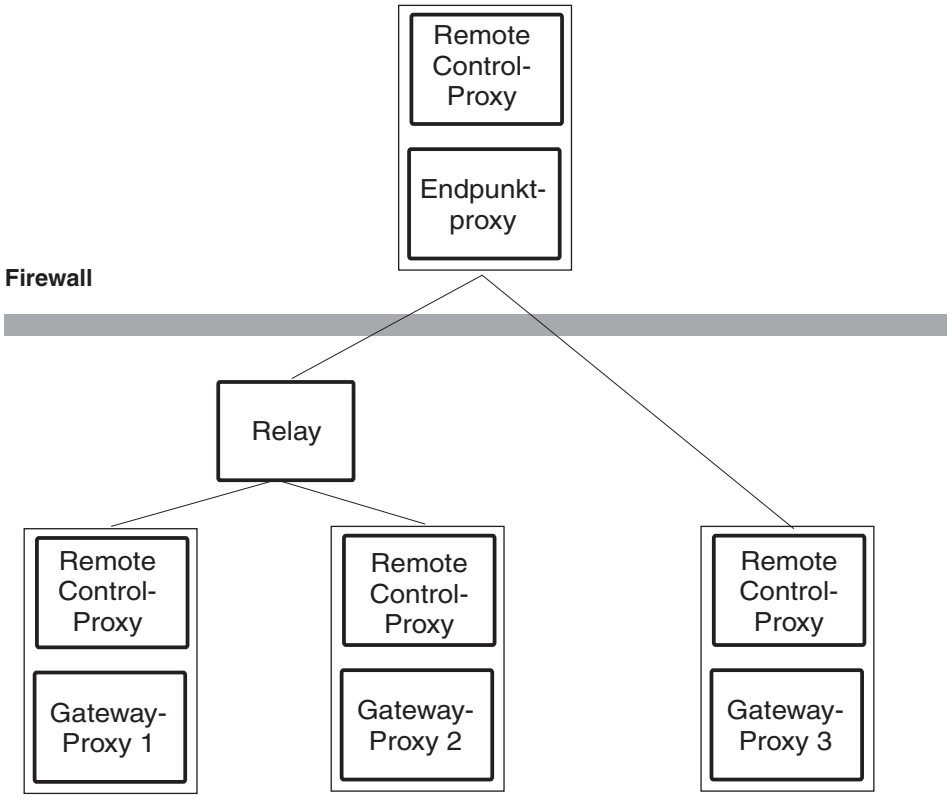
Mit Tivoli Firewall Security Toolbox arbeiten

Wenn Sie mit Tivoli Firewall Security Toolbox arbeiten, müssen Sie Folgendes definieren:

Übergeordneter Remote Control-Proxy
Der Remote Control-Proxy, der auf dem Endpunktproxyrechner ausgeführt wird. Dem Remote Control-Proxy können mehrere untergeordnete Elemente, Relay und untergeordnete Remote Control-Proxys zugeordnet werden.

Untergeordneter Remote Control-Proxy
Der Remote Control-Proxy, der auf dem Gateway-Proxyrechner ausgeführt wird. Dem untergeordneten Remote Control-Proxy kann nur ein einziges übergeordnetes Element zugeordnet werden: der übergeordnete Remote Control-Proxy oder ein Relay. Dem untergeordneten Remote Control-Proxy sind keine untergeordneten Elemente zugeordnet.

In der folgenden Abbildung sind die Rollen von untergeordneten und übergeordneten Remote Control-Proxys veranschaulicht.



- Der Remote Control-Proxy, der auf der Workstation mit dem Endpunktproxy installiert ist, verfügt über folgende untergeordnete Komponenten:
  - Relay. Das Relay ist dem Remote Control-Proxy, der auf dem Endpunktproxy ausgeführt wird, untergeordnet.
  - Remote Control-Proxy, der auf dem Rechner mit dem Gateway-Proxy 3 ausgeführt wird. Der Remote Control-Proxy ist dem Remote Control-Proxy, der auf dem Endpunktproxy ausgeführt wird, untergeordnet.
- Das Relay verfügt über folgende untergeordnete Komponenten:
  - Remote Control-Proxy, der auf dem Rechner mit dem Gateway-Proxy 1 ausgeführt wird. Der Remote Control-Proxy ist dem Relay untergeordnet.

– Remote Control-Proxy, der auf dem Rechner mit dem Gateway-Proxy 2 ausgeführt wird. Der Remote Control-Proxy ist dem Relay untergeordnet.

Mit Remote Control-Proxys im Standalone-Modus arbeiten

Wenn Sie mit Remote Control-Proxys im Standalone-Modus arbeiten, müssen Sie festlegen, welche Remote Control-Proxys übergeordnete bzw. untergeordnete Proxys sind. Um die Konfiguration zu optimieren, sollten Sie den Zielproxy als übergeordneten Proxy und den Controller-Proxy als untergeordneten Proxy definieren. Der Grund hierfür ist, dass der Zielproxy einigen Controllern zugeordnet ist und eine Verbindung zum Controller-Proxy herstellt, der mehreren Zielen zugeordnet ist.

Richtlinienmethode 'rc_def_proxy' für den Zielproxy konfigurieren

In den Richtlinienbereichen, in denen Sie Zielproxys verwenden, müssen Sie die Richtlinienmethode 'rc_def_proxy' wie folgt konfigurieren:

- Wenn der Zielproxy Tivoli Firewall Security Toolbox verwendet:

  `YES auto <Port des RC-Proxys>`

  Dabei steht <*Port des RC-Proxys*> für den Port, den alle Zielproxys verwenden müssen, um die Ziele zu emulieren.
- Für Zielproxys im Standalone-Modus:

  `YES manual <IP-Adresse des RC-Proxys> <Port des RC-Proxys>`

  Dabei gilt:

  <*IP-Adresse des RC-Proxys***>**
  Gibt die IP-Adresse des Rechners an, auf dem der Zielproxy ausgeführt wird.

  <*Port des RC-Proxys***>**
  Gibt den Port an, den alle Zielproxys verwenden müssen, um die Ziele zu emulieren.

Den Tivoli Remote Control-Proxy installieren

In diesem Abschnitt finden Sie Informationen zur Installation des Remote Control-Proxys als übergeordnetes oder untergeordnetes Element in einer der folgenden Umgebungen:

- Zusätzlich zu IBM Firewall Security Toolbox
- Im Standalone-Modus

Sie können die Remote Control-Proxys unter Verwendung der grafischen Benutzerschnittstelle oder einer Antwortdatei installieren.

Grafische Benutzerschnittstelle verwenden

Führen Sie zunächst folgende allgemeine Schritte aus:

1. Wechseln Sie vom Verzeichnis 'RCPROXY' in das Verzeichnis für die Plattform, auf der Sie den Proxy installieren möchten, und führen Sie das Installationsprogramm aus. Der InstallShield-Assistent zur Installation des Tivoli Remote Control-Proxys wird gestartet. Klicken Sie auf **Weiter**.
2. Klicken Sie im nächsten Dialog auf **Ja**, um die Lizenzvereinbarung zu akzeptieren.

3. Geben Sie im nächsten Dialog den Namen des Installationsverzeichnisses ein, und klicken Sie auf **Weiter**.

Welcher der vier Dialoge nachfolgend angezeigt wird, hängt davon ab, ob Sie den Remote Control-Proxy als übergeordnetes oder untergeordnetes Element zusätzlich zu Firewall Security Toolbox oder im Standalone-Modus installieren:

- „Übergeordneter Remote Control-Proxy zusätzlich zum Endpunktproxy"
- „Untergeordneter Remote Control-Proxy zusätzlich zum Gateway-Proxy" auf Seite 37
- „Übergeordneter Remote Control-Proxy im Standalone-Modus" auf Seite 40
- „Untergeordneter Remote Control-Proxy im Standalone-Modus" auf Seite 45

Anmerkung: In den Anzeigen des Assistenten, die in den folgenden Abschnitten beschrieben werden, sind zur Veranschaulichung Beispieldaten enthalten.

Übergeordneter Remote Control-Proxy zusätzlich zum Endpunktproxy

Wenn Sie den Remote Control-Proxy zusätzlich zu Tivoli Firewall Security Toolbox installieren, wird ein Dialog, der Sie über diese Umgebung informiert, angezeigt.

1. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:

Installation von IBM Tivoli Remote Control Proxy
Geben Sie die Portnummer des übergeordneten Remote Control-Proxys an, an dem er für Relay-Proxys oder untergeordnete Remote Control-Proxys empfangsbereit ist.
Geben Sie die Portnummer ein:
Lokaler Port, an dem dieser Proxy empfangsbereit ist:
7081
InstallShield
< Zurück
Weiter >
Abbrechen

2. Geben Sie die Portnummer des übergeordneten Remote Control-Proxys an, an dem er für Relay-Proxys oder untergeordnete Remote Control-Proxys empfangsbereit ist.

3. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:

Installation von IBM Tivoli Remote Control Proxy
Geben Sie die Liste der untergeordneten Hosts an, zu denen dieser Remote Control-Proxy eine Verbindung herstellt.
Netzwerkschnittstelle, an der der untergeordnete Proxy oder Relay-Proxy empfangsbereit ist:
Portnummer, an der der untergeordnete Proxy oder Relay-Proxy empfangsbereit ist:
Untergeordnete Hosts:
Hinzufügen
Entfernen
InstallShield
< Zurück
Weiter >
Abbrechen

4. Geben Sie in den folgenden Feldern Daten ein:

   Netzwerkschnittstelle, an der der untergeordnete Proxy oder Relay-Proxy empfangsbereit ist

   Geben Sie die Netzwerkschnittstelle (DNS-Name oder IP-Adresse) ein, an der der untergeordnete Remote Control-Proxy oder Relay-Proxy für Verbindungen vom übergeordneten Relay-Proxy oder Remote Control-Proxy empfangsbereit ist.

   Portnummer, an der der untergeordnete Proxy oder Relay-Proxy empfangsbereit ist

   Geben Sie die Portnummer ein, an der der untergeordnete Relay-Proxy oder Remote Control-Proxy für Verbindungen mit dem übergeordneten Relay-Proxy oder Remote Control-Proxy empfangsbereit ist.

5. Klicken Sie auf **Hinzufügen**, um den untergeordneten Remote Control-Proxy zur Liste hinzuzufügen.
6. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:

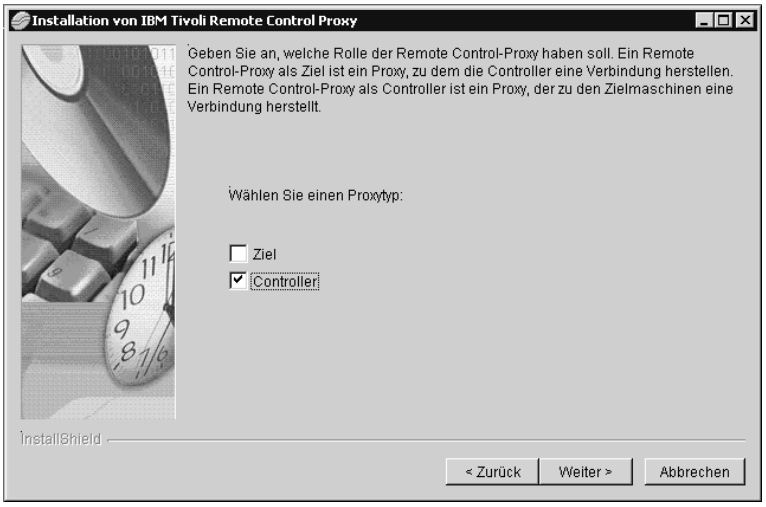
Installation von IBM Tivoli Remote Control Proxy
Definieren Sie, wie die Verbindungen zwischen diesem Proxy und seinem übergeordneten Proxy oder Relay-Proxy gestartet werden. Bidirektional: Sowohl dieser Proxy als auch der übergeordnete Proxy bzw. Relay-Proxy können die Verbindung starten. Unidirektional: Nur dieser Proxy oder sein übergeordneter Proxy bzw. Relay-Proxy können die Verbindung starten.
Verbindungsart:
Bidirektional
Unidirektional
Unidirektionale Rolle:
Auslöser
Empfänger
InstallShield
< Zurück
Weiter >
Abbrechen

7. Definieren Sie, wie die Verbindungen zwischen diesem Proxy und seinem untergeordneten Proxy oder Relay-Proxy gestartet werden:
   - Wählen Sie **Bidirektional** aus, um Verbindungen zuzulassen, die von beiden Rechnern initiiert wurden.
   - Wählen Sie **Unidirektional** aus, um Verbindungen zuzulassen, die nur von einem Rechner initiiert wurden.

     Bei Auswahl dieser Option müssen Sie eine der folgende Optionen auswählen:

     Auslöser
     Startet die Verbindung mit dem untergeordneten Proxy oder Relay-Proxy

     Empfänger
     Ist für untergeordneten Proxy oder Relay-Proxy empfangsbereit.
8. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:


Installation von IBM Tivoli Remote Control Proxy
Geben Sie an, welche Rolle der Remote Control-Proxy haben soll. Ein Remote Control-Proxy als Ziel ist ein Proxy, zu dem die Controller eine Verbindung herstellen. Ein Remote Control-Proxy als Controller ist ein Proxy, der zu den Zielmaschinen eine Verbindung herstellt.
Wählen Sie einen Proxytyp:
Ziel
Controller
InstallShield
< Zurück
Weiter >
Abbrechen

9. Wählen Sie eine oder beide Rollen für den Remote Control-Proxy aus, und klicken Sie auf **Weiter**. Wenn Sie **Ziel** ausgewählt haben, wird der folgende Dialog angezeigt. Andernfalls wird der Dialog unter Schritt 11 auf Seite 37 angezeigt.

Installation von IBM Tivoli Remote Control Proxy
Geben Sie den Port an, an dem dieser Proxy für Verbindungen von Controllern und Controller-Proxys empfangsbereit ist. Die angegebene Portnummer muss mit dem in der Richtlinienmethode rc_def_proxy definierten Wert übereinstimmen.
Portnummer:
3501
InstallShield
< Zurück
Weiter >
Abbrechen

10. Geben Sie die Portnummer an, an dem dieser Proxy für Verbindungen von Controllern und Controller-Proxys empfangsbereit ist. Die Portnummer muss dem in der Richtlinie 'rc_def_proxy' angegebenen Wert entsprechen (siehe „Richtlinienmethode 'rc_def_proxy' für den Zielproxy konfigurieren" auf Seite 33).
11. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:

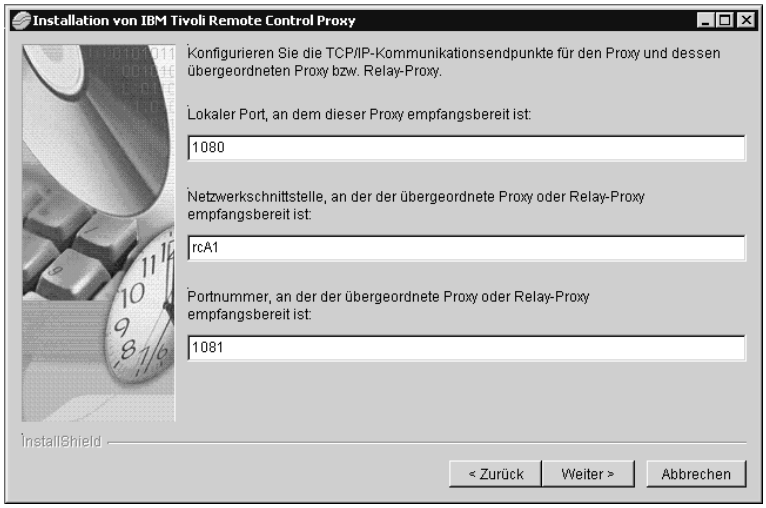
Installation von IBM Tivoli Remote Control Proxy
Geben Sie die Portnummer für die Befehlszeile an, an der dieser Proxy für Anforderungen empfangsbereit ist.
Geben Sie die Portnummer ein:
Portnummer für die Befehlszeile:
5555
InstallShield
< Zurück
Weiter >
Abbrechen

12. Geben Sie die Portnummer an, an der dieser Proxy für Anforderungen über die Befehlszeile empfangsbereit ist.
13. Klicken Sie auf **Weiter**. Im nächsten Dialog wird eine Zusammenfassung Ihrer Eingaben angezeigt.
14. Klicken Sie auf **Zurück**, wenn Sie Ihre Einstellungen ändern möchten. Andernfalls klicken Sie auf **Weiter**, um fortzufahren. Die Installation des Remote Control-Proxys wird fortgesetzt.

Untergeordneter Remote Control-Proxy zusätzlich zum Gateway-Proxy

Wenn Sie den Remote Control-Proxy zusätzlich zu Tivoli Firewall Security Toolbox installieren, wird ein Dialog, der Sie über diese Umgebung informiert, angezeigt.

1. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:


Installation von IBM Tivoli Remote Control Proxy
Konfigurieren Sie die TCP/IP-Kommunikationsendpunkte für den Proxy und dessen übergeordneten Proxy bzw. Relay-Proxy.
Lokaler Port, an dem dieser Proxy empfangsbereit ist:
1080
Netzwerkschnittstelle, an der der übergeordnete Proxy oder Relay-Proxy empfangsbereit ist:
rcA1
Portnummer, an der der übergeordnete Proxy oder Relay-Proxy empfangsbereit ist:
1081
InstallShield
< Zurück
Weiter >
Abbrechen

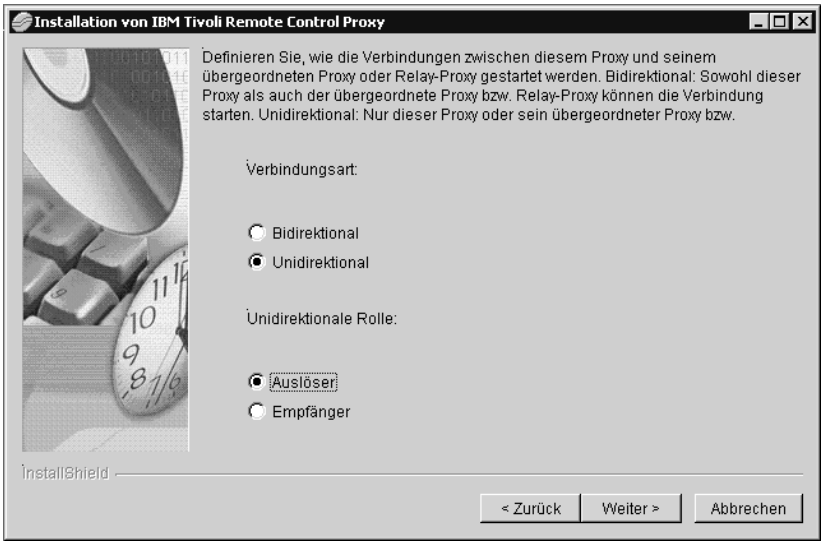
2. Geben Sie in den folgenden Feldern Daten ein:

   Lokaler Port, an dem dieser Proxy empfangsbereit ist
   Geben Sie die Portnummer ein, an der der untergeordnete Remote Control-Proxy für Verbindungen mit seinem übergeordneten Relay-Proxy oder Remote Control-Proxy empfangsbereit ist.

   Netzwerkschnittstelle, an der der übergeordnete Proxy oder Relay-Proxy empfangsbereit ist
   Geben Sie die Netzwerkschnittstelle (DNS-Name oder IP-Adresse) ein, an der der übergeordnete Remote Control-Proxy oder Relay-Proxy für Verbindungen vom untergeordneten Relay-Proxy oder Remote Control-Proxy empfangsbereit ist.

   Portnummer, an der der übergeordnete Proxy oder Relay-Proxy empfangsbereit ist
   Geben Sie die Portnummer ein, an der der übergeordnete Relay-Proxy oder Remote Control-Proxy für Verbindungen mit seinen untergeordneten Relay-Proxys oder Remote Control-Proxys empfangsbereit ist.

3. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:


Installation von IBM Tivoli Remote Control Proxy
Definieren Sie, wie die Verbindungen zwischen diesem Proxy und seinem übergeordneten Proxy oder Relay-Proxy gestartet werden. Bidirektional: Sowohl dieser Proxy als auch der übergeordnete Proxy bzw. Relay-Proxy können die Verbindung starten. Unidirektional: Nur dieser Proxy oder sein übergeordneter Proxy bzw.
Verbindungsart:
Bidirektional
Unidirektional
Unidirektionale Rolle:
Auslöser
Empfänger
InstallShield
< Zurück
Weiter >
Abbrechen

4. Definieren Sie, wie die Verbindungen zwischen diesem Proxy und seinem übergeordneten Proxy oder Relay-Proxy gestartet werden.
   - Wählen Sie **Bidirektional** aus, um Verbindungen zuzulassen, die von beiden Rechnern initiiert wurden.
   - Wählen Sie **Unidirektional** aus, um Verbindungen zuzulassen, die nur von einem Rechner initiiert wurden.

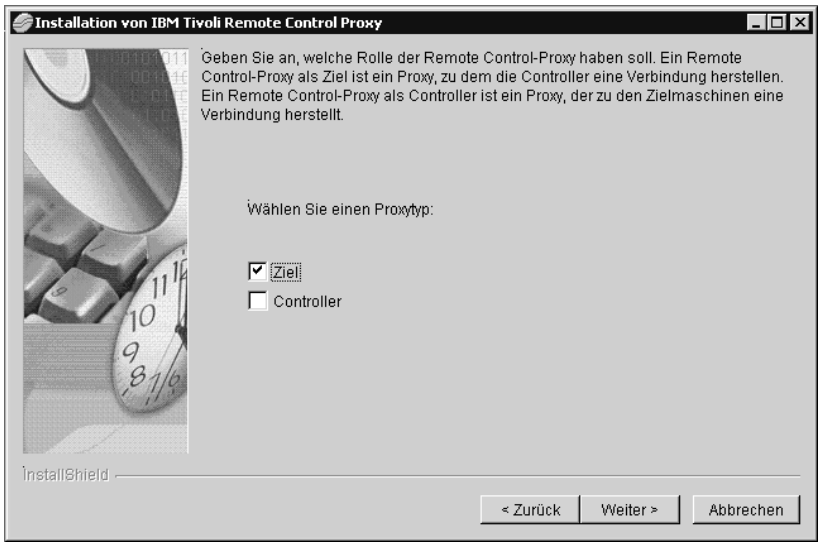
     Bei Auswahl dieser Option müssen Sie eine der folgende Optionen auswählen:

     Auslöser
     Startet die Verbindung mit dem übergeordneten Proxy oder Relay-Proxy.

     Empfänger
     Ist für übergeordneten Proxy oder Relay-Proxy empfangsbereit.

Untergeordneter Remote Control-Proxy zusätzlich zum Gateway-Proxy

5. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:


Installation von IBM Tivoli Remote Control Proxy
Geben Sie an, welche Rolle der Remote Control-Proxy haben soll. Ein Remote Control-Proxy als Ziel ist ein Proxy, zu dem die Controller eine Verbindung herstellen. Ein Remote Control-Proxy als Controller ist ein Proxy, der zu den Zielmaschinen eine Verbindung herstellt.
Wählen Sie einen Proxytyp:
Ziel
Controller
InstallShield
< Zurück
Weiter >
Abbrechen

6. Wählen Sie die Roll(e) des Remote Control-Proxys aus, und klicken Sie auf **Weiter**. Wenn Sie **Ziel** ausgewählt haben, wird der folgende Dialog angezeigt. Andernfalls wird der Dialog unter Schritt 8 auf Seite 40 angezeigt.

Installation von IBM Tivoli Remote Control Proxy
Geben Sie den Port an, an dem dieser Proxy für Verbindungen von Controllern und Controller-Proxys empfangsbereit ist. Die angegebene Portnummer muss mit dem in der Richtlinienmethode rc_def_proxy definierten Wert übereinstimmen.
Portnummer:
3501
InstallShield
< Zurück
Weiter >
Abbrechen

7. Geben Sie den Port an, an dem dieser Proxy für Verbindungen von Controllern und Controller-Proxys empfangsbereit ist. Die Portnummer muss dem in der Richtlinie 'rc_def_proxy' angegebenen Wert entsprechen (siehe „Richtlinienmethode 'rc_def_proxy' für den Zielproxy konfigurieren" auf Seite 33).

Untergeordneter Remote Control-Proxy zusätzlich zum Gateway-Proxy

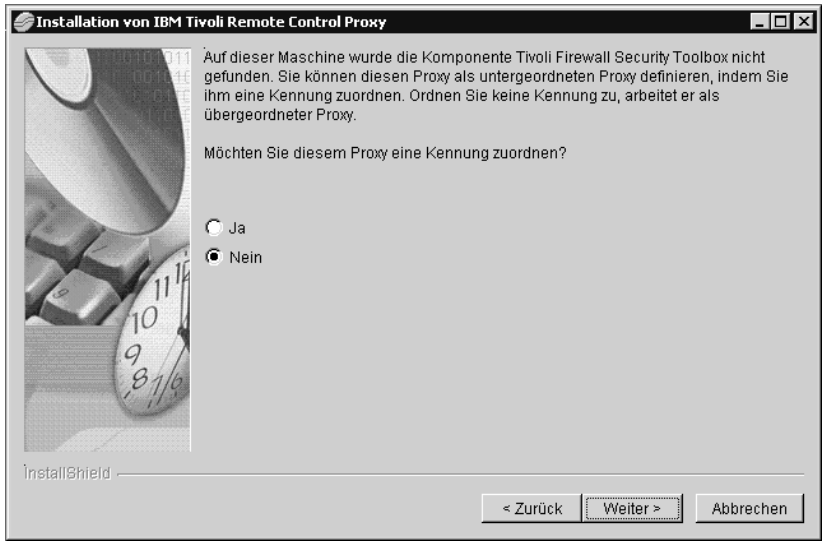
8. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:

Installation von IBM Tivoli Remote Control Proxy
Geben Sie die Portnummer für die Befehlszeile an, an der dieser Proxy für Anforderungen empfangsbereit ist.
Geben Sie die Portnummer ein:
Portnummer für die Befehlszeile:
5555
InstallShield
< Zurück
Weiter >
Abbrechen

9. Geben Sie die Portnummer an, an der dieser Proxy für Anforderungen über die Befehlszeile empfangsbereit ist.
10. Klicken Sie auf **Weiter**. Im nächsten Dialog wird eine Zusammenfassung Ihrer Eingaben angezeigt.
11. Klicken Sie auf **Zurück**, wenn Sie Ihre Einstellungen ändern möchten. Klicken Sie andernfalls auf **Weiter**, um den Remote Control-Proxy zu installieren.

Übergeordneter Remote Control-Proxy im Standalone-Modus

Bei der Installation des Remote Control-Proxys im Standalone-Modus wird folgender Dialog angezeigt:


Installation von IBM Tivoli Remote Control Proxy
Auf dieser Maschine wurde die Komponente Tivoli Firewall Security Toolbox nicht gefunden. Sie können diesen Proxy als untergeordneten Proxy definieren, indem Sie ihm eine Kennung zuordnen. Ordnen Sie keine Kennung zu, arbeitet er als übergeordneter Proxy.
Möchten Sie diesem Proxy eine Kennung zuordnen?
Ja
Nein
InstallShield
< Zurück
Weiter >
Abbrechen

1. Wählen Sie **Nein** aus, und klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:

Installation von IBM Tivoli Remote Control Proxy
Geben Sie die Portnummer des übergeordneten Remote Control-Proxys an, an dem er für Relay-Proxys oder untergeordnete Remote Control-Proxys empfangsbereit ist.
Geben Sie die Portnummer ein:
Lokaler Port, an dem dieser Proxy empfangsbereit ist:
7081
InstallShield
< Zurück
Weiter >
Abbrechen

2. Geben Sie die Portnummer des übergeordneten Remote Control-Proxys an, an dem er für Relay-Proxys oder untergeordnete Remote Control-Proxys empfangsbereit ist.
3. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:

Installation von IBM Tivoli Remote Control Proxy
Geben Sie die Liste der untergeordneten Hosts an, zu denen dieser Remote Control-Proxy eine Verbindung herstellt.
Netzwerkschnittstelle, an der der untergeordnete Proxy oder Relay-Proxy empfangsbereit ist:
Portnummer, an der der untergeordnete Proxy oder Relay-Proxy empfangsbereit ist:
Untergeordnete Hosts:
Hinzufügen
Entfernen
InstallShield
< Zurück
Weiter >
Abbrechen

4. Geben Sie in den folgenden Feldern Daten ein:

   Netzwerkschnittstelle, an der der untergeordnete Proxy oder Relay-Proxy empfangsbereit ist

   Geben Sie die Netzwerkschnittstelle (DNS-Name oder IP-Adresse) ein, an der der untergeordnete Remote Control-Proxy oder Relay-Proxy für Verbindungen vom übergeordneten Relay-Proxy oder Remote Control-Proxy empfangsbereit ist.

Portnummer, an der der untergeordnete Proxy oder Relay-Proxy empfangsbereit ist

Geben Sie die Portnummer ein, an der der untergeordnete Relay-Proxy oder Remote Control-Proxy für Verbindungen mit dem übergeordneten Relay-Proxy oder Remote Control-Proxy empfangsbereit ist.

5. Klicken Sie auf **Hinzufügen**, um den untergeordneten Remote Control-Proxy zur Liste hinzuzufügen.
6. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:

Installation von IBM Tivoli Remote Control Proxy
Definieren Sie, wie die Verbindungen zwischen diesem Proxy und seinem übergeordneten Proxy oder Relay-Proxy gestartet werden. Bidirektional: Sowohl dieser Proxy als auch der übergeordnete Proxy bzw. Relay-Proxy können die Verbindung starten. Unidirektional: Nur dieser Proxy oder sein übergeordneter Proxy bzw. Relay-Proxy können die Verbindung starten.
Verbindungsart:
Bidirektional
Unidirektional
Unidirektionale Rolle:
Auslöser
Empfänger
InstallShield
< Zurück
Weiter >
Abbrechen

7. Definieren Sie, wie die Verbindungen zwischen diesem Proxy und seinem untergeordneten Proxy oder Relay-Proxy gestartet werden:
   - Wählen Sie **Bidirektional** aus, um Verbindungen zuzulassen, die von beiden Rechner initiiert wurden.
   - Wählen Sie **Unidirektional** aus, um Verbindungen zuzulassen, die nur von einem Rechner initiiert wurden.

     Bei Auswahl dieser Option müssen Sie eine der folgende Optionen auswählen:

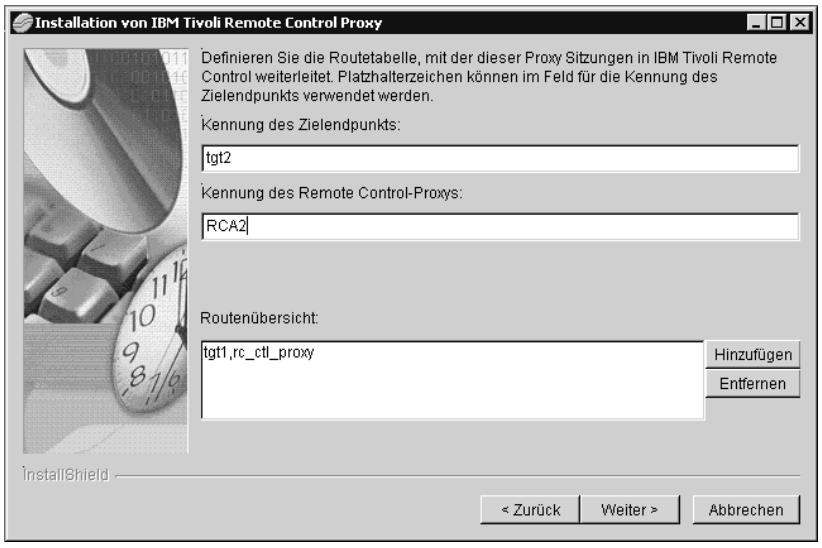
     Auslöser

     Startet die Verbindung mit dem untergeordneten Proxy oder Relay-Proxy

     Empfänger

     Ist für untergeordneten Proxy oder Relay-Proxy empfangsbereit.

8. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:

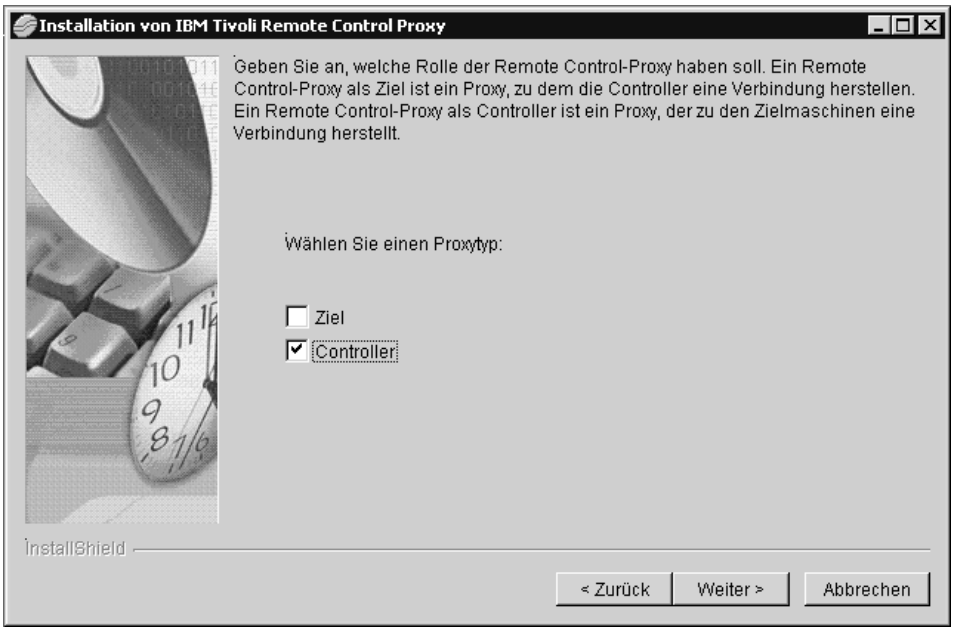

Installation von IBM Tivoli Remote Control Proxy
Definieren Sie die Routetabelle, mit der dieser Proxy Sitzungen in IBM Tivoli Remote Control weiterleitet. Platzhalterzeichen können im Feld für die Kennung des Zielendpunkts verwendet werden.
Kennung des Zielendpunkts:
tgt2
Kennung des Remote Control-Proxys:
RCA2
Routenübersicht:
tgt1,rc_ctl_proxy
Hinzufügen
Entfernen
InstallShield
< Zurück
Weiter >
Abbrechen

9. Geben Sie in den folgenden Feldern Daten ein:

   Kennung des Zielendpunkts
   Geben Sie die Kennung eines Zielrechners ein.

   Kennung des Remote Control-Proxys
   Geben Sie die Kennung des Controller-Proxys ein, der mit dem angegebenen Zielrechner verbunden ist.

10. Klicken Sie auf **Hinzufügen**, um die Kennung des Zielrechners und die Kennung des verbundenen Controller-Proxys zur Liste mit den Remote Control-Proxys hinzuzufügen. Diese Daten werden in der Datei 'rcproxy.route', die sich im Installationsverzeichnis für den Remote Control-Proxy befindet, gespeichert. Weitere Informationen finden Sie unter „Den Pfad für untergeordnete Proxys in Szenarios mit dem Remote Control-Proxy im Standalone-Modus definieren" auf Seite 58.
11. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:


Installation von IBM Tivoli Remote Control Proxy
Geben Sie an, welche Rolle der Remote Control-Proxy haben soll. Ein Remote Control-Proxy als Ziel ist ein Proxy, zu dem die Controller eine Verbindung herstellen. Ein Remote Control-Proxy als Controller ist ein Proxy, der zu den Zielmaschinen eine Verbindung herstellt.
Wählen Sie einen Proxytyp:
Ziel
Controller
InstallShield
< Zurück
Weiter >
Abbrechen

12. Wählen Sie die Rolle(n) des Remote Control-Proxys aus, und klicken Sie auf **Weiter**. Wenn Sie **Ziel** ausgewählt haben, wird der folgende Dialog angezeigt. Andernfalls wird der Dialog unter Schritt 14 angezeigt.

Installation von IBM Tivoli Remote Control Proxy
Geben Sie den Port an, an dem dieser Proxy für Verbindungen von Controllern und Controller-Proxys empfangsbereit ist. Die angegebene Portnummer muss mit dem in der Richtlinienmethode rc_def_proxy definierten Wert übereinstimmen.
Portnummer:
3501
InstallShield
< Zurück
Weiter >
Abbrechen

13. Geben Sie den Port an, an dem dieser Proxy für Verbindungen von Controllern und Controller-Proxys empfangsbereit ist. Die Portnummer muss dem in der Richtlinie 'rc_def_proxy' angegebenen Wert entsprechen (siehe „Richtlinienmethode 'rc_def_proxy' für den Zielproxy konfigurieren" auf Seite 33).
14. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:

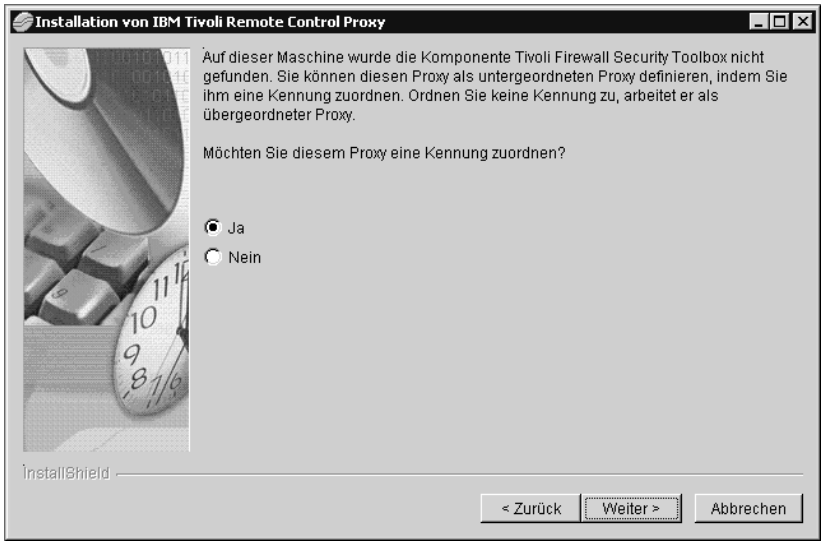
Installation von IBM Tivoli Remote Control Proxy
Geben Sie die Portnummer für die Befehlszeile an, an der dieser Proxy für Anforderungen empfangsbereit ist.
Geben Sie die Portnummer ein:
Portnummer für die Befehlszeile:
5555
InstallShield
< Zurück
Weiter >
Abbrechen

15. Geben Sie die Portnummer an, an der dieser Proxy für Anforderungen über die Befehlszeile empfangsbereit ist.

16. Klicken Sie auf **Weiter**. Im nächsten Dialog wird eine Zusammenfassung Ihrer Eingaben angezeigt.
17. Klicken Sie auf **Zurück**, wenn Sie Ihre Einstellungen ändern möchten. Klicken Sie andernfalls auf **Weiter**, um den Remote Control-Proxy zu installieren.

Untergeordneter Remote Control-Proxy im Standalone-Modus

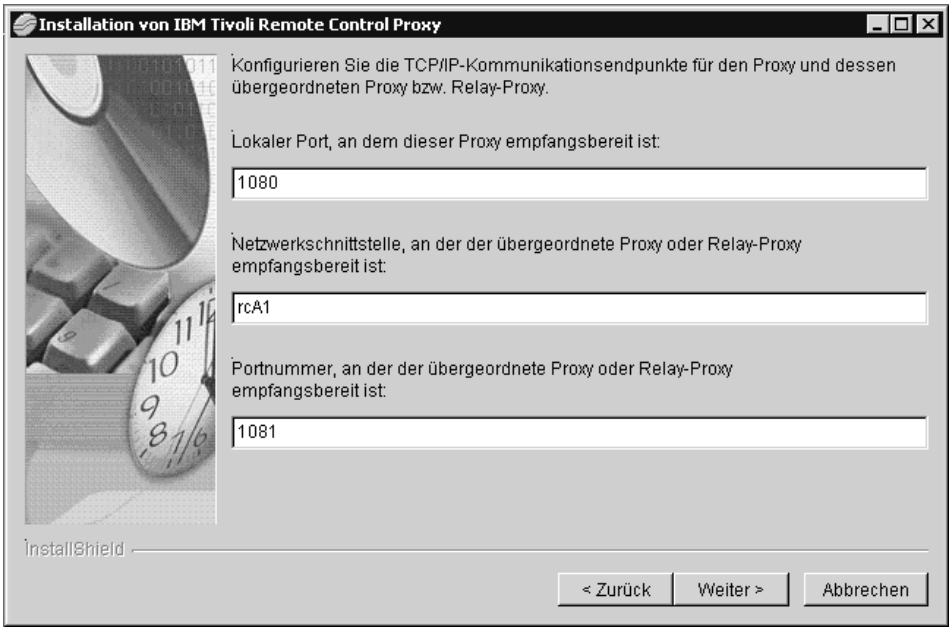
Bei der Installation des Remote Control-Proxys im Standalone-Modus wird folgender Dialog angezeigt:


Installation von IBM Tivoli Remote Control Proxy
Auf dieser Maschine wurde die Komponente Tivoli Firewall Security Toolbox nicht gefunden. Sie können diesen Proxy als untergeordneten Proxy definieren, indem Sie ihm eine Kennung zuordnen. Ordnen Sie keine Kennung zu, arbeitet er als übergeordneter Proxy.
Möchten Sie diesem Proxy eine Kennung zuordnen?
Ja
Nein
InstallShield
< Zurück
Weiter >
Abbrechen

1. Wählen Sie **Ja** zum Definieren einer Kennung für den Remote Control-Proxy aus, und klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:

2. Geben Sie einen Namen zur Kennzeichnung des Remote Control-Proxys ein, und klicken Sie auf **Weiter**.

   Daraufhin wird folgender Dialog angezeigt:


Installation von IBM Tivoli Remote Control Proxy
Konfigurieren Sie die TCP/IP-Kommunikationsendpunkte für den Proxy und dessen übergeordneten Proxy bzw. Relay-Proxy.
Lokaler Port, an dem dieser Proxy empfangsbereit ist:
1080
Netzwerkschnittstelle, an der der übergeordnete Proxy oder Relay-Proxy empfangsbereit ist:
rcA1
Portnummer, an der der übergeordnete Proxy oder Relay-Proxy empfangsbereit ist:
1081
InstallShield
< Zurück
Weiter >
Abbrechen

3. Geben Sie in den folgenden Feldern Daten ein:

   Lokaler Port, an dem dieser Proxy empfangsbereit ist
   Geben Sie die Portnummer ein, an dem der untergeordnete Remote Control-Proxy für Verbindungen mit seinem übergeordneten Relay-Proxy oder Remote Control-Proxy empfangsbereit ist.

   Netzwerkschnittstelle, an der der übergeordnete Proxy oder Relay-Proxy empfangsbereit ist
   Geben Sie die Netzwerkschnittstelle (DNS-Name oder IP-Adresse) ein, an der der übergeordnete Remote Control-Proxy oder Relay-Proxy für Verbindungen vom untergeordneten Relay-Proxy oder Remote Control-Proxy empfangsbereit ist.

   Portnummer, an der der übergeordnete Proxy oder Relay-Proxy empfangsbereit ist
   Geben Sie die Portnummer ein, an der der übergeordnete Relay-Proxy oder Remote Control-Proxy für Verbindungen mit seinen untergeordneten Relay-Proxys oder Remote Control-Proxys empfangsbereit ist.

4. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:

Installation von IBM Tivoli Remote Control Proxy
Definieren Sie, wie die Verbindungen zwischen diesem Proxy und seinem übergeordneten Proxy oder Relay-Proxy gestartet werden. Bidirektional: Sowohl dieser Proxy als auch der übergeordnete Proxy bzw. Relay-Proxy können die Verbindung starten. Unidirektional: Nur dieser Proxy oder sein übergeordneter Proxy bzw.
Verbindungsart:
Bidirektional
Unidirektional
Unidirektionale Rolle:
Auslöser
Empfänger
InstallShield
< Zurück
Weiter >
Abbrechen

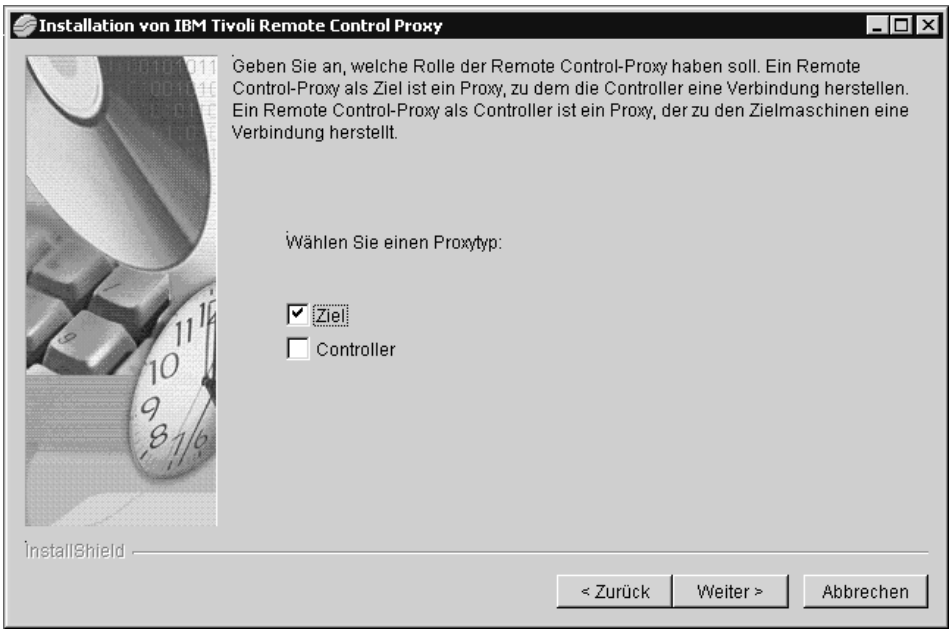
5. Definieren Sie, wie die Verbindungen zwischen diesem Proxy und seinem übergeordneten Proxy oder Relay-Proxy gestartet werden.
   - Wählen Sie **Bidirektional** aus, um Verbindungen zuzulassen, die von beiden Rechner initiiert wurden.
   - Wählen Sie **Unidirektional** aus, um Verbindungen zuzulassen, die nur von einem Rechner initiiert wurde.

     Bei Auswahl dieser Option müssen Sie eine der folgende Optionen auswählen:

     Auslöser
     Startet die Verbindung mit dem übergeordneten Proxy oder Relay-Proxy.

     Empfänger
     Ist für übergeordneten Proxy oder Relay-Proxy empfangsbereit.

6. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:


Installation von IBM Tivoli Remote Control Proxy
Geben Sie an, welche Rolle der Remote Control-Proxy haben soll. Ein Remote Control-Proxy als Ziel ist ein Proxy, zu dem die Controller eine Verbindung herstellen. Ein Remote Control-Proxy als Controller ist ein Proxy, der zu den Zielmaschinen eine Verbindung herstellt.
Wählen Sie einen Proxytyp:
Ziel
Controller
InstallShield
< Zurück
Weiter >
Abbrechen

7. Wählen Sie die Rolle(n) des Remote Control-Proxys aus, und klicken Sie auf **Weiter**. Wenn Sie **Ziel** ausgewählt haben, wird der folgende Dialog angezeigt. Andernfalls wird der Dialog unter Schritt 9 auf Seite 49 angezeigt.

Installation von IBM Tivoli Remote Control Proxy
Geben Sie den Port an, an dem dieser Proxy für Verbindungen von Controllern und Controller-Proxys empfangsbereit ist. Die angegebene Portnummer muss mit dem in der Richtlinienmethode rc_def_proxy definierten Wert übereinstimmen.
Portnummer:
3501
InstallShield
< Zurück
Weiter >
Abbrechen

8. Geben Sie die Portnummer an, an dem dieser Proxy für Verbindungen von Controllern und Controller-Proxys empfangsbereit ist. Die Portnummer muss dem in der Richtlinie 'rc_def_proxy' angegebenen Wert entsprechen (siehe „Richtlinienmethode 'rc_def_proxy' für den Zielproxy konfigurieren" auf Seite 33).

9. Klicken Sie auf **Weiter**. Daraufhin wird folgender Dialog angezeigt:

Installation von IBM Tivoli Remote Control Proxy
Geben Sie die Portnummer für die Befehlszeile an, an der dieser Proxy für Anforderungen empfangsbereit ist.
Geben Sie die Portnummer ein:
Portnummer für die Befehlszeile:
5555
InstallShield
< Zurück
Weiter >
Abbrechen

10. Geben Sie die Portnummer an, an der dieser Proxy für Anforderungen über die Befehlszeile empfangsbereit ist.
11. Klicken Sie auf **Weiter**. Im nächsten Dialog wird eine Zusammenfassung Ihrer Eingaben angezeigt.
12. Klicken Sie auf **Zurück**, wenn Sie Ihre Einstellungen ändern möchten. Klicken Sie andernfalls auf **Weiter**, um den Remote Control-Proxy zu installieren.

Antwortdatei verwenden

Sie können für den Remote Control-Proxy eine automatische Installation durchführen. Bei der automatischen Installation liest der Installationsprozess die Informationen aus der Antwortdatei. Benutzereingaben sind dabei nicht erforderlich.

Führen Sie hierfür folgende Schritte aus:

1. Passen Sie eine der folgenden Antwortdateien an, die sich im Verzeichnis 'new\RCPROXY' der IBM Tivoli Remote Control-CD befinden:

Name der Antwortdatei	Beschreibung
epp.rsp	Verwenden Sie diese Antwortdatei, wenn der Endpunktproxy bereits auf der Workstation, auf der Sie den Remote Control-Proxy installieren möchten, installiert ist.
gwp.rsp	Verwenden Sie diese Antwortdatei, wenn der Gateway-Proxy bereits auf der Workstation, auf der Sie den Remote Control-Proxy installieren möchten, installiert ist.
stdl_epp.rsp	Verwenden Sie diese Antwortdatei, wenn weder der Endpunktproxy noch der Gateway-Proxy auf der Workstation, auf der Sie den Remote Control-Proxy installieren möchten, installiert sind und wenn dem Remote Control-Proxy die Rolle 'übergeordnet' zugeordnet werden muss.

Remote Control-Proxy im Standalone-Modus

Name der Antwortdatei	Beschreibung
stdl_gwp.rsp	Verwenden Sie diese Antwortdatei, wenn weder der Endpunktproxy noch der Gateway-Proxy auf der Workstation, auf der Sie den Remote Control-Proxy installieren möchten, installiert sind und wenn dem Remote Control-Proxy die Rolle 'untergeordnet' zugeordnet werden muss.

Einträge in den Antwortdateien haben folgendes Format:

```
Schlüsselwort=Wert
```

Anmerkung: Nachdem Sie die Antwortdatei editiert haben, müssen Sie sicherstellen, dass nach dem letzten Eintrag keine Leerzeilen eingefügt sind.

2. Legen Sie den Datenträger für die Installation des Remote Control-Proxys in ein Laufwerk ein, auf das die Systeme, auf denen Sie die automatische Installation des Remote Control-Proxys durchführen möchten, über einen Laufwerkbuchstaben zugreifen können.
3. Installieren Sie den Remote Control-Proxy, indem Sie folgenden Befehl ausführen:
   - Unter Windows 2000:

     ```
     setup.exe -is:silent -silent -options
     <Absoluter Pfad>\<Name der Antwortdatei>.rsp
     ```

   - Unter Linux, AIX und Solaris:

     ```
     install.sh -is:silent -silent -options
     <Absoluter Pfad>/<Name der Antwortdatei>.rsp
     ```

Das Relay installieren

Führen Sie zur Installation des Relays die im Handbuch *Tivoli Management Framework: Firewall Security Toolbox User's Guide* beschriebenen Schritte aus. Wenden Sie die in der folgenden Tabelle angegebene Regel an:

Wenn das Installationsprogramm Informationen anfordert	Stellen Sie diese Informationen zur Verfügung
`Relay- oder Endpunktproxy`	Der übergeordnete Relay-Proxy oder Remote Control-Proxy
`Relay- oder Gateway-Proxy`	Der untergeordnete Relay-Proxy oder Remote Control-Proxy

Bei Verwendung von Tivoli Firewall Security Toolbox zur Kommunikation über Firewalls müssen Sie sicherstellen, dass auf allen Relay-Rechnern zwei Relay-Instanzen installiert sind. Eine Instanz ist für die Kommunikation mit dem Endpunktproxy, dem Gateway-Proxy bzw. dem Relay-Proxy erforderlich, die andere Instanz wird für die Kommunikation mit den Remote Control-Proxys benötigt. Führen Sie hierzu die im Handbuch *Tivoli Management Framework: Firewall Security Toolbox User's Guide* beschriebenen Schritte aus.

Den Remote Control-Proxy konfigurieren

Nach Abschluss der Installation des Remote Control-Proxys wird die Konfigurationsdatei 'rcproxy.cfg' im Installationsverzeichnis erstellt. In dieser Datei sind die Konfigurationsdaten, die Sie während der Installation eingeben, enthalten. Sie können auch andere Optionen konfigurieren. Zum Ändern dieser Daten oder Konfigurieren anderer Optionen müssen Sie die Datei 'rcproxy.cfg' mit einem Texteditor editieren.

Stoppen und starten Sie den Remote Control-Proxy neu, um Ihre Änderungen zu aktivieren. Informationen zum Stoppen bzw. Starten des Remote Control-Proxys finden Sie unter „rcproxy" auf Seite 150.

Die Abschnitte der Konfigurationsdatei werden im Folgenden beschrieben. Jeder Abschnitt enthält eine Tabelle mit Schlüsselwörtern und Beschreibungen. Geben Sie die Werte in folgendem Format ein:

Schlüsselwort=Wert

Bei den Abschnittstiteln muss die Groß-/Kleinschreibung nicht beachtet werden.

Log (übergeordneter und untergeordneter Remote Control-Proxy)

Im Abschnitt [log] sind die Protokolloptionen aufgelistet. Die Schüsselwörter werden in der folgenden Tabelle beschrieben.

Schlüsselwort	Beschreibung
debug-level	Die Detaillierungsebene im Protokoll. Die Ebenen 0 und 1 werden für Standardoperationen empfohlen. Ebenen höher als 3 sollten nur verwendet werden, wenn dies von der Tivoli-Kundenunterstützung zur Diagnose von Fehlern empfohlen wird. Die Auswahl einer Ebene höher als 6 wirkt sich auf die Leistung des Services aus und sollte mit Vorsicht verwendet werden. Gültiger Bereich: 0-11. Der Standardwert ist 3.
log-file	Der vollständige Pfad für die Protokolldatei, in die der Remote Control-Proxy Nachrichten schreibt. Der Standardwert ist 'rcproxy.log'. Wenn Sie keine Datei angeben, ist der Standardwert die Standardfehlerausgabe.
max-size	Die maximale Größe (in MB) einer Protokolldatei. Wenn die Protokolldatei ihre maximale Größe erreicht, wird sie in *Dateiname*.log.bak umbenannt, und es wird eine neue Protokolldatei gestartet. Wenn Sie die maximale Größe nicht beschränken möchten, geben Sie 0 an. Der Standardwert ist 1.

Communication-layer (übergeordneter Remote Control-Proxy)

Im Abschnitt [communication-layer] sind Optionen für Verbindungen zwischen dem übergeordneten Remote Control-Proxy und den untergeordneten Relay-Proxys bzw. Remote Control-Proxys aufgelistet. Die Schüsselwörter werden in der folgenden Tabelle beschrieben.

Schlüsselwort	Beschreibung
children-local-host	Die Netzwerkschnittstelle (DNS-Name oder IP-Adresse), an der der übergeordnete Remote Control-Proxy für untergeordnete Relay-Proxys oder Remote Control-Proxys empfangsbereit ist.

Abschnitt 'Communication-layer'

Schlüsselwort	Beschreibung
children-local-port	Die Portnummer, an der der übergeordnete Remote Control-Proxy für untergeordnete Relay-Proxys oder Remote Control-Proxys empfangsbereit ist. Dieses Schlüsselwort ist obligatorisch.
children-remote-list	Die Liste mit untergeordneten Hosts (Relay-Proxys oder Remote Control-Proxys), zu denen der übergeordnete Remote Control-Proxy eine Verbindung herstellt. Trennen Sie die Eingaben durch ein Semikolon (;). Am Ende der Zeile darf kein Begrenzer eingefügt werden. Beispiel: Ein Relay mit der Adresse 192.168.99.71 und der Portnummer 7071 und ein untergeordneter Remote Control-Proxy mit der Adresse 192.168.99.80 und der Portnummer 7073: `192.168.99.71+7071;192.168.99.80+7073` Dieses Schlüsselwort ist obligatorisch.
children-cm-type	Die Verbindungsrichtung (unidirektional oder bidirektional), die bei der Kommunikation des übergeordneten Remote Control-Proxys mit seinen untergeordneten Relay-Proxys bzw. Remote Control-Proxys zur Anwendung kommt. Gültige Werte: cm-tcp-bidirectional, cm-tcp-unidirectional. Dieses Schlüsselwort ist obligatorisch.
buffer-size	Die Anzahl von Peernachrichten in falscher Reihenfolge, die vom Remote Control-Proxy zwischengespeichert werden. Gültiger Bereich: 4, 1024. Der Standardwert ist 8. Um die Netzwerkleistung zu optimieren, können Sie den Remote Control-Proxy so konfigurieren, dass er Nachrichten sendet, ohne eine Bestätigung vom fernen Peer abzuwarten (hierzu müssen Sie den Wert für 'use-rsm-reply' im Abschnitt 'rcproxy' auf 0 setzen). Bei dieser Konfiguration kann es sein, dass die Nachrichten den fernen Peer in der falschen Reihenfolge erreichen. Ist dies der Fall, stellt der ferne Peer die Nachrichten in eine interne Warteschlange und bringt sie in die richtige Reihenfolge. Die Länge dieser Warteschlange, d. h. die maximale Anzahl von Nachrichten in falscher Reihenfolge, die vom Proxy verwaltet werden können, wird über den Parameter 'buffer-size' konfiguriert.

Folgender Abschnitt ist beispielsweise möglich:

```
[communication-layer]
children-local-host=LAB001
children-local-port=7081
children-remote-list=LAB002+7080
children-cm-type=cm-tcp-unidirectional
```

Communication-layer (untergeordneter Remote Control-Proxy)

Im Abschnitt [communication-layer] sind Optionen für Verbindungen zwischen dem untergeordneten Remote Control-Proxy und dem übergeordneten Relay-Proxy bzw. Remote Control-Proxy aufgelistet. Die Schüsselwörter werden in der folgenden Tabelle beschrieben.

Schlüsselwort	Beschreibung
parent-local-host	Die Netzwerkschnittstelle (DNS-Name oder IP-Adresse) ein, an der der untergeordnete Remote Control-Proxy für den übergeordneten Relay-Proxy oder Remote Control-Proxy empfangsbereit ist.
parent-local-port	Die Portnummer, an der der untergeordnete Remote Control-Proxy für den übergeordneten Relay-Proxy bzw. Remote Control-Proxy empfangsbereit ist. Dieses Schlüsselwort ist obligatorisch.
parent-remote-host	Die Netzwerkschnittstelle (DNS-Name oder IP-Adresse) des übergeordneten Hosts (Relay-Proxy oder Remote Control-Proxy).
parent-remote-port	Die Portnummer, an der der übergeordnete Relay-Proxy oder Remote Control-Proxy für Verbindungen mit seinen untergeordneten Relay-Proxys oder Remote Control-Proxys empfangsbereit ist. Dieses Schlüsselwort ist obligatorisch.
parent-cm-type	Die Verbindungsrichtung (unidirektional oder bidirektional), die bei der Kommunikation des untergeordneten Remote Control-Proxys mit seinem übergeordneten Relay-Proxy bzw. Remote Control-Proxy zur Anwendung kommt. Gültige Werte: cm-tcp-bidirectional, cm-tcp-unidirectional. Dieses Schlüsselwort ist obligatorisch.
buffer-size	Die Anzahl von Peernachrichten in falscher Reihenfolge, die vom Remote Control-Proxy zwischengespeichert werden. Gültiger Bereich: 4, 1024. Der Standardwert ist 8. Um die Netzwerkleistung zu optimieren, können Sie den Remote Control-Proxy so konfigurieren, dass er Nachrichten sendet, ohne eine Bestätigung vom fernen Peer abzuwarten (hierzu müssen Sie den Wert für 'use-rsm-reply' im Abschnitt 'rcproxy' auf 0 setzen). Bei dieser Konfiguration kann es sein, dass die Nachrichten den fernen Peer in der falschen Reihenfolge erreichen. Ist dies der Fall, stellt der ferne Peer die Nachrichten in eine interne Warteschlange und bringt sie in die richtige Reihenfolge. Die Länge dieser Warteschlange, d. h. die maximale Anzahl von Nachrichten in falscher Reihenfolge, die vom Proxy verwaltet werden können, wird über den Parameter 'buffer-size' konfiguriert.

Folgender Abschnitt ist beispielsweise möglich:

```
[communication-layer]
parent-local-host=LAB002
parent-local-port=7080
parent-remote-host=LAB001
parent-remote-port=7081
parent-cm-type=cm-tcp-unidirectional
```

Children-cm-info (Übergeordneter Remote Control-Proxy)

Im Abschnitt [children-cm-info] sind weitere Optionen für die Konnektivität des übergeordneten Remote Control-Proxys und der untergeordneten Relay-Proxys oder Remote Control-Proxys aufgelistet. Die Schüsselwörter werden in der folgenden Tabelle beschrieben.

Schlüsselwort	Beschreibung
connection-mode	Die Rolle des übergeordneten Remote Control-Proxys (gilt nur für unidirektionale Verbindungen). Gültige Werte: **initiator** Die Maschine, die die Verbindung startet. Normalerweise ist dies der Rechner auf der sicheren Seite. **listener** Die Maschine, die empfangsbereit ist. Normalerweise ist dies der Rechner auf der ungeschützten Seite. Der Standardwert ist 'listener'. Dieses Schlüsselwort ist obligatorisch.
local-port-range	Der Bereich der lokalen Ports, der zum Herstellen einer Verbindung zu einem anderen Peer verwendet wird. Beispiel: Ports 6060, 7000 bis 7070, 9050 und 8000 bis 8080: `6060,7000-7070,9050,8000-8080`
receive-buffer-size	Die Größe (in Kilobyte) des Puffers, der für den Empfang von TCP/IP-Stackverbindungen verwendet wird. Der Mindestwert beträgt 1. Der Standardwert ist 17.
connect-timeout	Das Zeitlimit (in Sekunden), nach dessen Ablauf ein TCP/IP-Verbindungsvorgang fehlschlägt. Geben Sie den Wert 0 an, um das Zeitlimit zu deaktivieren und den Standardwert der TCP/IP-Bibliothek zu verwenden.
send-timeout	Das Zeitlimit (in Sekunden), nach dessen Ablauf ein TCP/IP-Sendevorgang fehlschlägt. Geben Sie den Wert 0 an, um das Zeitlimit zu deaktivieren. Der Standardwert ist 120.
log-mode	Der Puffer, der während einer Peerverbindung gesendet bzw. empfangen wird. Die Leistung wird möglicherweise beeinträchtigt, wenn Sie einen anderen Wert als 0 angeben. Werte: 0=keinen Puffer 1=nur gesendete Daten 2=nur empfangene Daten 3=alle übertragenen Daten. Der Standardwert ist 0.
drop-timeout	Gilt nur für bidirektionale Verbindungen. Das Zeitlimit (inSekunden), nach dessen Ablauf eine inaktive Sitzung geschlossen wird. Geben Sie den Wert 0 an, um die Verbindung zu schließen, sobald der Nutzungszähler den Wert 0 erreicht. Der Standardwert ist 5.
polling-interval	Gilt nur für auslösende Komponenten im Falle von unidirektionalen Verbindungen. Der Initiator sendet in regelmäßigen Abständen eine Abfrage an den Empfänger, um zu prüfen, ob er eine Verbindung herstellen muss. Diese Option ist das Intervall (in Sekunden), nach dessen Ablauf der Initiator automatisch eine Verbindung zum Empfänger herstellt. Der Standardwert ist 2.

Schlüsselwort	Beschreibung
drop-interval	Gilt nur für Empfängerkomponenten im Falle von unidirektionalen Verbindungen. Gibt das Intervall (in Sekunden) an, nach dessen Ablauf der Empfänger eine inaktive Verbindung aussetzt. Der Standardwert ist 5.

Folgender Abschnitt ist beispielsweise möglich:

```
[children-cm-info]
connection-mode=initiator
```

Parent-cm-info (Untergeordneter Remote Control-Proxy)

Im Abschnitt [parent-cm-info] sind weitere Optionen für die Konnektivität des untergeordneten Remote Control-Proxys und des übergeordneten Relay-Proxys oder Remote Control-Proxys aufgelistet. Die Schlüsselwörter, die Sie in diesem Abschnitt verwenden können, stimmen mit den für den Abschnitt [parent-cm-info] beschriebenen Schlüsselwörtern überein.

Folgender Abschnitt ist beispielsweise möglich:

```
[parent-cm-info]
connection-mode=listener
```

Rcproxy (Übergeordneter und untergeordneter Remote Control-Proxy)

Im Abschnitt [rcproxy] sind die Hauptoptionen für den Remote Control-Proxy aufgelistet. Die Schüsselwörter werden in der folgenden Tabelle beschrieben.

Schlüsselwort	Beschreibung
proxy-label	Die Kennung zur Identifikation des Remote Control-Proxys. Das Schlüsselwort ist in den folgenden Szenarios obligatorisch: • Der Remote Control-Proxy wird auf der Maschine mit dem Gateway-Proxy ausgeführt. Während der Installation des Remote Control-Proxys wird dieses Schlüsselwort automatisch auf die Kennung des Gateway-Proxys gesetzt. Das Schlüsselwort sollte nicht geändert werden. • Der Remote Control-Proxy im Standalone-Modus muss als untergeordneter Proxy ausgeführt werden. Wenn Sie dem Remote Control-Proxy keine Kennung zuweisen, wird er als übergeordneter Proxy ausgeführt. Standardwert: *Hostname*.
proxy-type	Die Rollen der Remote Control-Proxys. Gültige Werte: **controller** Der Remote Control-Proxy, der als Controller eine Verbindung zum Zielrechner herstellt. **target** Der Remote Control-Proxy, der als Zielrechner mit dem Controller verbunden ist. **both** Der Remote Control-Proxy, der als Controller oder Ziel ausgeführt werden kann.
proxy-port	Der Port des Zielproxys, an dem er für den Controller und den Controller-Proxy empfangsbereit ist. Die Portnummer muss mit dem in der Richtlinienmethode 'rc_def_proxy' angegebenen Wert übereinstimmen. Standardwert: 9494.
proxy-interface	Diese Option wird für Remote Control-Proxys verwendet, die über mehr als eine Netzwerkschnittstelle und Adresse verfügen. Sie ist die DNS- oder IP-Adresse der Netzwerkschnittstelle, an der der Zielproxy für Controller bzw. Controller-Proxys empfangsbereit ist. Die Angabe dieses Parameters ist nur dann obligatorisch, wenn für den Parameter 'proxy-type' der Wert **target** oder **both** angegeben wurde.
comm-timeout	Das Zeitlimit (in Sekunden), nach dessen Ablauf der TCP/IP-Vorgang fehlschlägt. Dieser Parameter steuert eingehende und abgehende Verbindungen zwischen dem Proxy und seinem übergeordneten Proxy oder Endpunkten. Mit diesem Zeitlimit wird eine Überlastung des Proxys durch Denial-of-Service-Attacken von Clients, die Verbindungen öffnen, jedoch nicht schließen, verhindert. Der Standardwert ist 240.
cmdline-port	Der Port des Remote Control-Proxys, an dem er für Befehle über die Befehlszeile empfangsbereit ist. Die Angabe dieses Parameters, für den es keinen Standardwert gibt, ist obligatorisch.

Schlüsselwort	Beschreibung
epp-directory	Das Verzeichnis, in dem der Endpunktproxy installiert ist. Dieses Schlüsselwort muss zur Konfiguration des übergeordneten Remote Control-Proxys verwendet werden. Wenn Sie keinen Wert für diesen Parameter angeben, wird der Remote Control-Proxy im Standalone-Modus ausgeführt.
max-sessions	Die Anzahl der Verbindungen, die vom Remote Control-Proxy gleichzeitig gesteuert werden können. Der Standardwert ist 10.
use-rsm-reply	Dieser Parameter verbessert die Leistung und sollte nur geändert werden, wenn dies von der Kundenunterstützung empfohlen wird. Der Parameterwert muss für beide Remote Control-Proxys identisch sein. Mögliche Werte sind: **0** Wenn Sie keine Relays verwenden. **1** Wenn Sie Relays verwenden. Standardwert: 0.

Folgende Abschnitte sind beispielsweise möglich:

- Wenn Sie mit Tivoli Firewall Security Toolbox arbeiten und die Maschine mit dem übergeordneten Remote Control-Proxy konfigurieren:

```
[rcproxy]
proxy-type=target
proxy-port=9494
proxy-interface=LAB001
cmdline-port=9999
epp-directory=<Installationsverzeichnis für Endpunktproxy>
```

- Wenn Sie mit Tivoli Firewall Security Toolbox arbeiten und die Maschine mit dem untergeordneten Remote Control-Proxy konfigurieren:

```
[rcproxy]
proxy-label=<Kennung des Gateway-Proxys>
proxy-type=controller
cmdline-port=9999
```

- Wenn Sie mit dem Remote Control-Proxy im Standalone-Modus arbeiten und die Maschine mit dem übergeordneten Remote Control-Proxy konfigurieren:

```
[rcproxy]
proxy-type=target
proxy-port=9494
proxy-interface=LAB001
cmdline-port=9999
```

- Wenn Sie mit dem Remote Control-Proxy im Standalone-Modus arbeiten und die Maschine mit dem untergeordneten Remote Control-Proxy konfigurieren:

```
[rcproxy]
proxy-type=controller
cmdline-port=9999
```

Den Pfad für untergeordnete Proxys in Szenarios mit dem Remote Control-Proxy im Stand-alone-Modus definieren

Nach der Installation des übergeordneten Remote Control-Proxys in einer Standalone-Umgebung wird die Konfigurationsdatei `rcproxy.route` im Installationsverzeichnis erstellt. Diese Datei enthält Informationen zum untergeordneten Proxy, der eine Sitzung mit dem Ziel startet. Diese Daten haben Sie während der Installation eingegeben.

Um diese Daten zu ändern, müssen Sie die Datei `rcproxy.route` mit einem Texteditor editieren. Sie müssen in jeder Zeile der Datei `rcproxy.route` die Kennung des Zielrechners und die Kennung des verbundenen, untergeordneten Proxys eingeben. Trennen Sie die Kennungen durch ein Komma. Es dürfen keine Leerzeichen verwendet werden. Bei der Angabe der Kennungen können folgende Platzhalterzeichen verwendet werden:

***** Steht für eine beliebige Zeichenfolge.

? Steht für ein beliebiges Einzelzeichen.

Im Folgenden wird ein Beispiel für die Datei `rcproxy.route` angezeigt:

```
#
# This file contains static routing table information
# for the Remote Control proxy
#
# Each line specifies an endpoint (target) label and the label
# of the controller proxy that serves it, separated by a comma like this:
#
# endpoint_label,proxy_label
#
# When you specify a label you can use the following
# wildcard characters:
# asterisk (*)      to match any string
# question mark (?) to match any character
#
f???o,foo_proxy
z*,any_proxy
y*,bar_proxy
```

Anmerkung: Wenn zu Ihrer Umgebung nur eine Tivoli Management Region gehört, darf die Datei 'rcproxy.route' nur folgenden Zeile enthalten:

**,Proxykennung*

Dabei steht *Proxykennung* für den Namen des untergeordneten Controller-Proxys.

Ein Beispielszenario

In diesem Abschnitt wird ein Beispielszenario für ein Unternehmen beschrieben, das Tivoli Remote Control verwendet, um seinen Kunden IT-Services außerhalb des eigenen Unternehmens zur Verfügung zu stellen. Der Help-Desk des Unternehmens muss sich des öffentlich zugänglichen Netzwerkbereichs bedienen, um auf Kundendomänen zugreifen zu können und Fehler im Kundennetzwerk zu beheben. Für die Konfiguration dieser Umgebung ist das Verständnis und die Planung der Netzwerktopologie unbedingt erforderlich.

Unternehmensweite Architektur

Die unternehmensweite Architektur setzt sich aus drei virtuellen Teilnetzen zusammen: aus zwei Teilnetzen im Intranetnetzwerk und einem Teilnetz in der DMZ-Umgebung (DMZ = Demilitarized Zone).

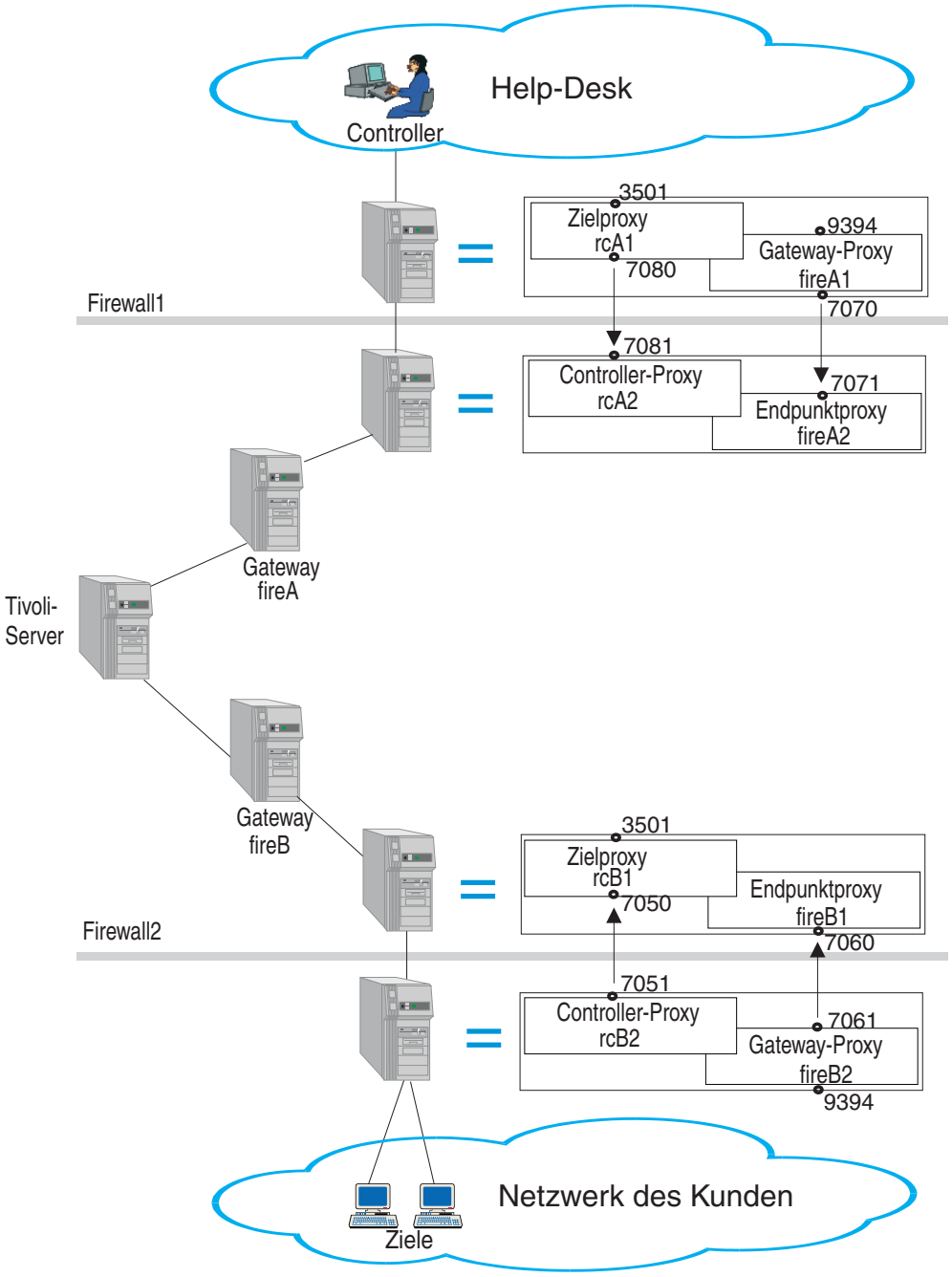
Das Help-Desk-Teilnetz und das Kundenteilnetz befinden sich auf der geschützten Seite des Netzwerks. Die Controller befinden sich im Help-Desk-Teilnetz und die zu überwachenden Ziele im Kundenteilnetz. Die Tivoli-Server gehören zum Serverteilnetz, das sich in der DMZ-Umgebung befindet.

Die Kunden des Unternehmens und Outsourcer schützen Ihre Netzwerke, indem Sie Firewalls einsetzen, die den Aufbau von Verbindungen steuern.

Je nach Position der Firewall müssen die Outsourcer die Proxykomponenten von Remote Control installieren. Da die Firewalls die Tivoli-Management-Gateways und die Endpunkte voneinander trennen, müssen Sie die Remote Control-Proxys zusammen mit den Komponenten von Firewall Security Toolbox verwenden.

In der folgenden Abbildung ist die Unternehmensumgebung und die Position der Firewalls und folglich der Proxys dargestellt.

Die folgenden Abschnitte enthalten die Parameter für die Basiskonfiguration, die Sie während des Installationsprozesses setzen können und die in den Konfigurationsdateien der Endpunktproxys, Gateway-Proxys und Remote Control-Proxys gespeichert werden. Sie können Parameter für die erweiterte Konfiguration angeben (beispielsweise für Maschinen, die über mehreren Netzwerkschnittstellen und Adressen verfügen), indem Sie die textbasierten Konfigurationsdateien editieren.



Firewall-Konnektivität

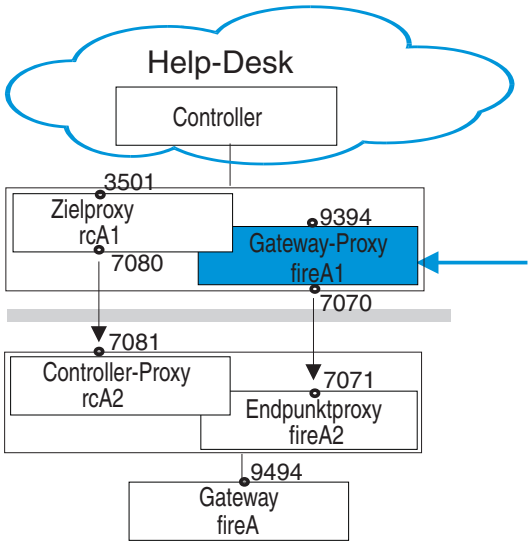
Vor der Konfiguration der Proxys müssen Sie den Konnektivitätstyp, den die Firewalls verwenden, ermitteln. Wenn beispielsweise die Firewalls in diesem Szenario unidirektionale Verbindungen zulassen, müssen Sie sicherstellen, dass die Firewalls Verbindungen an den definierten Ports gemäß dem folgenden Schema zulassen.

- Firewall1 muss folgende Verbindungen zulassen:
  - An Port 7071 zwischen fireA1 und fireA2
  - An Port 7081 zwischen rcA1 und rcA2
- Firewall2 muss folgende Verbindungen zulassen:
  - An Port 7060 zwischen fireB2 und fireB1
  - An Port 7050 zwischen rcB2 und rcB1

Gateway-Proxy fireA1

Die Konfigurationsdatei 'gwproxy.cfg' des Gateway-Proxys, die sich im Installationsverzeichnis des Gateway-Proxys befindet, sollte folgende Informationen enthalten:

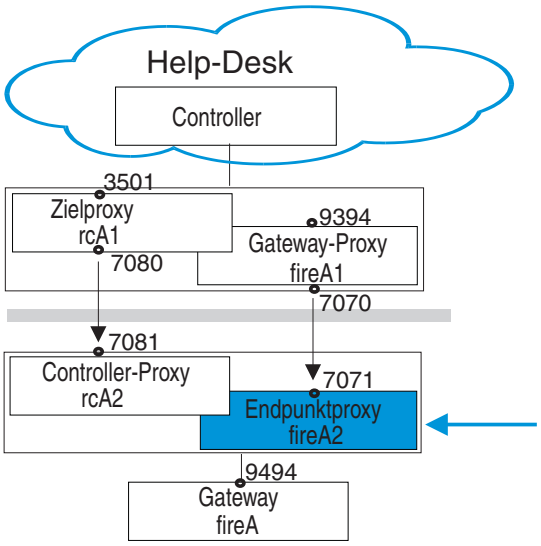
```
[gateway-proxy]
gateway-port = 9394
proxy-label = fireA1
[communication-layer]
parent-local-host = fireA1
parent-local-port = 7070
parent-remote-host = fireA2
parent-remote-port = 7071
parent-cm-type = cm-tcp-unidirectional
[parent-cm-info]
connection-mode = initiator
```



Endpunktproxy fireA2

Die Konfigurationsdatei 'epproxy.cfg' des Endpunktproxys, die sich im Installationsverzeichnis des Endpunktproxys befindet, sollte folgende Informationen enthalten:

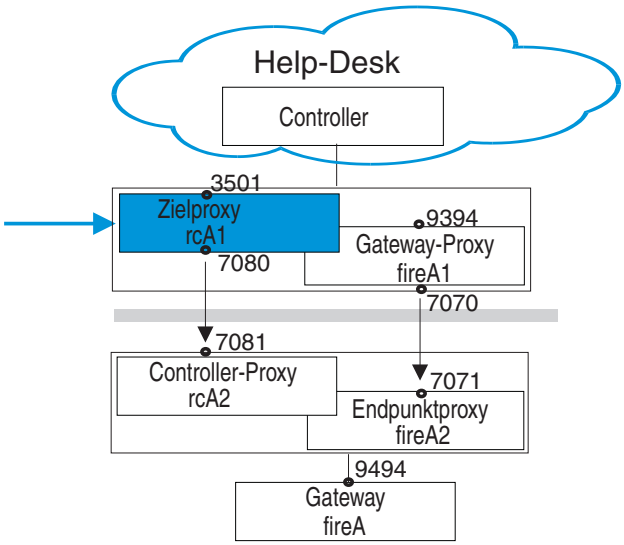
```
[endpoint-proxy]
gateway-host = fireA+9494
[communication-layer]
children-local-host = fireA2
children-local-port = 7071
children-remote-list = fireA1+7070
children-cm-type = cm-tcp-unidirectional
[children-cm-info]
connection-mode = listener
```



Zielproxy rcA1

Die Konfigurationsdatei 'rcproxy.cfg' des Zielproxys, die sich im Installationsverzeichnis des Zielproxys befindet, sollte folgende Informationen enthalten:

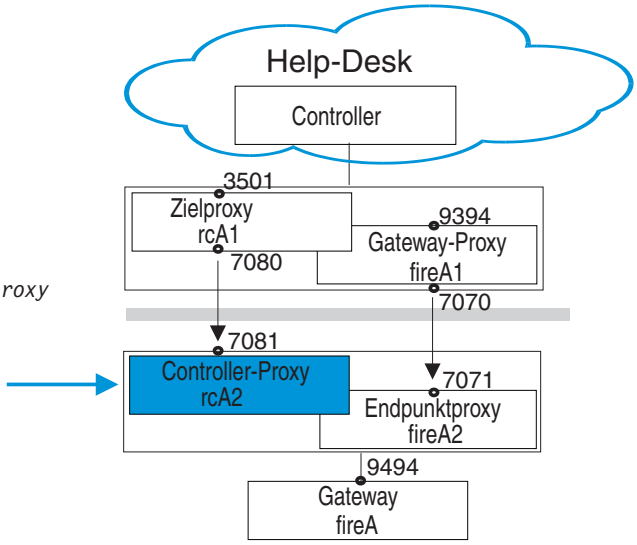
```
[communication-layer]
parent-local-host = rcA1
parent-local-port = 7080
parent-remote-host = rcA2
parent-remote-port = 7081
parent-cm-type = cm-tcp-unidirectional
[parent-cm-info]
connection-mode = initiator
[rcproxy]
proxy-label = fireA1
proxy-type = target
proxy-port = 3501
proxy-interface = rcA1
cmdline-port = 9999
```



Controller-Proxy rcA2

Die Konfigurationsdatei 'rcproxy.cfg' des Controller-Proxys, die sich im Installationsverzeichnis des Controller-Proxys befindet, sollte folgende Informationen enthalten:

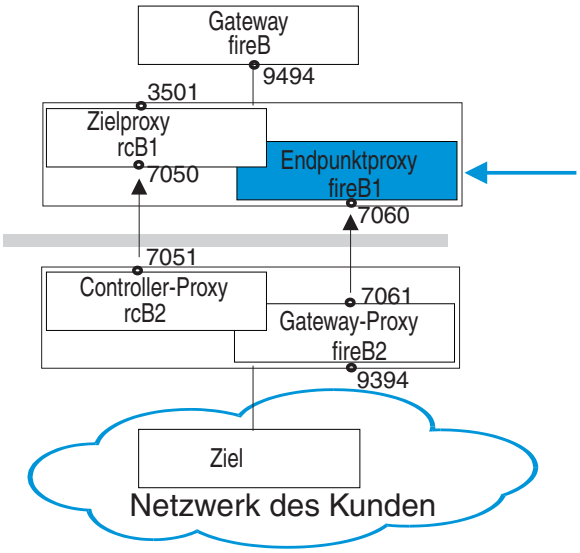
```
[communication-layer]
children-local-host = rcA2
children-local-port = 7081
children-remote-list = rcA1+7080
children-cm-type = cm-tcp-unidirectional
[children-cm-info]
connection-mode = listener
[rcproxy]
proxy-type = controller
cmdline-port = 9999
epp-directory = Installationsverzeichnis für Endpunktproxy
```



Endpunktproxy fireB1

Die Konfigurationsdatei 'epproxy.cfg' des Endpunktproxys, die sich im Installationsverzeichnis des Endpunktproxys befindet, sollte folgende Informationen enthalten:

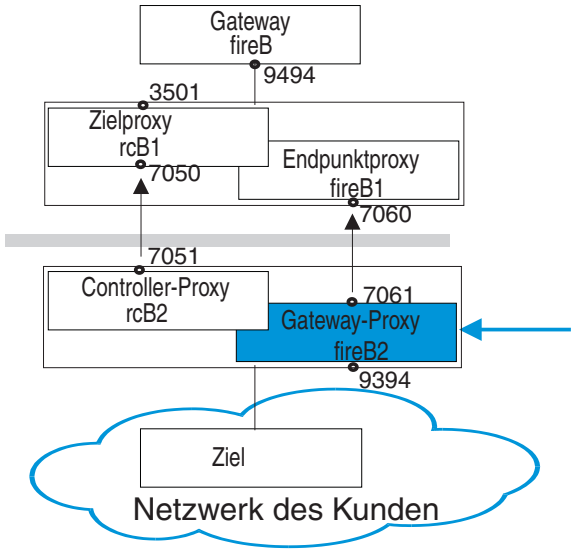
```
[endpoint-proxy]
gateway-host = fireB+9494
[communication-layer]
children-local-host = fireB1
children-local-port = 7060
children-remote-list = fireB2+7061
children-cm-type = cm-tcp-unidirectional
[children-cm-info]
connection-mode = listener
```



Gateway-Proxy fireB2

Die Konfigurationsdatei 'gwproxy.cfg' des Gateway-Proxys, die sich im Installationsverzeichnis des Gateway-Proxys befindet, sollte folgende Informationen enthalten:

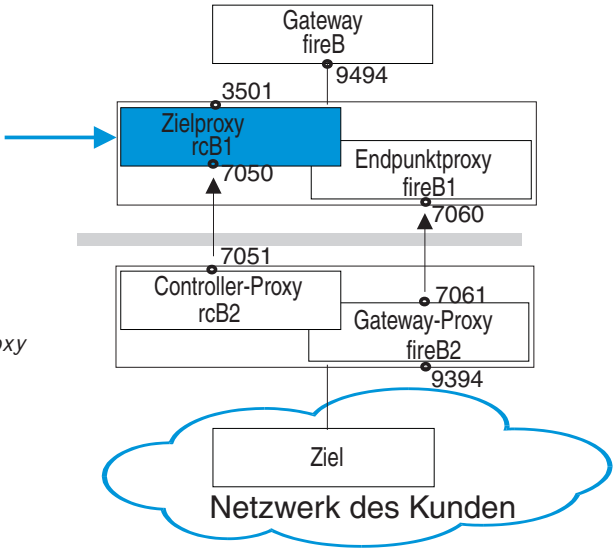
```
[gateway-proxy]
gateway-port = 9394
proxy-label = fireB2
[communication-layer]
parent-local-host = fireB2
parent-local-port = 7061
parent-remote-host = fireB1
parent-remote-port = 7060
parent-cm-type = cm-tcp-unidirectional
[parent-cm-info]
connection-mode = initiator
```



Zielproxy rcB1

Die Konfigurationsdatei 'rcproxy.cfg' des Zielproxys, die sich im Installationsverzeichnis des Zielproxys befindet, sollte folgende Informationen enthalten:

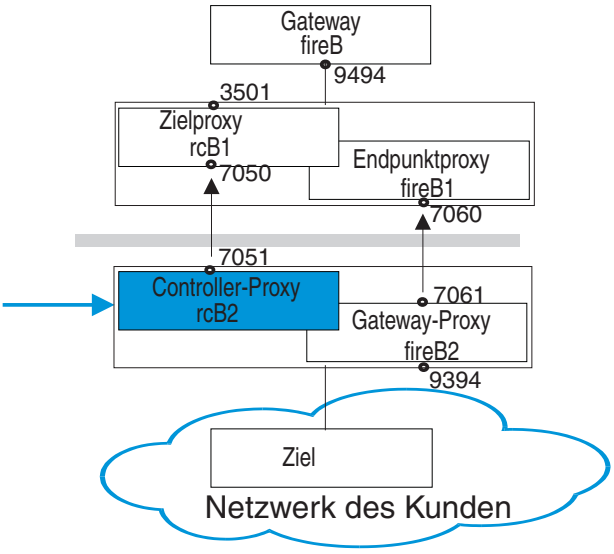
```
[communication-layer]
children-local-host = rcB1
children-local-port = 7050
children-remote-list = rcB2+7051
children-cm-type = cm-tcp-unidirectional
[children-cm-info]
connection-mode = listener
[rcproxy]
proxy-type = target
proxy-port = 3501
proxy-interface = rcB1
cmdline-port = 9999
epp-directory = Installationsverzeichnis für Endpunktproxy
```



Controller-Proxy rcB2

Die Konfigurationsdatei 'rcproxy.cfg' des Controller-Proxys, die sich im Installationsverzeichnis des Controller-Proxys befindet, sollte folgende Informationen enthalten:

```
[communication-layer]
parent-local-host = rcB2
parent-local-port = 7051
parent-remote-host = rcB1
parent-remote-port = 7050
parent-cm-type = cm-tcp-unidirectional
[parent-cm-info]
connection-mode = initiator
[rcproxy]
proxy-label = fireB2
proxy-type = controller
cmdline-port = 9999
```



Kapitel 4. Die Tivoli-Umgebung für die Verwendung der Tivoli Remote Control-Schnittstellen konfigurieren

Bevor Sie die Tivoli Remote Control-Schnittstellen verwenden können, müssen Sie zunächst die Tivoli-Umgebung konfigurieren. Führen Sie hierzu folgende Tasks aus:

- Fernverbindungen des Tivoli-Servers aktivieren.
- Speziellen Tivoli-Administrator definieren. Dies ist nur für die Webschnittstelle erforderlich.

Fernverbindungen aktivieren

Bevor Sie eine Verbindung zwischen dem Tivoli-Desktop bzw. der Webschnittstelle und einem Tivoli-Server mit Tivoli Management Framework 4.1 herstellen, müssen Sie sicherstellen, dass der Tivoli-Server Fernverbindungen unterstützt. Um festzustellen, ob es fernen Systemen möglich ist, sich am Tivoli-Server anzumelden, verwenden Sie den Befehl **odadmin** auf dem Hostrechner. Wenn der Befehl **odadmin** die folgende Nachricht zurückgibt, ist die Anmeldung durch ferne Systeme nicht möglich:

```
Ferne Clientanmeldung zulässig =FALSE
```

Um Fernverbindungen zu aktivieren, müssen Sie die Option **Ferne Clientanmeldung zulässig** auf **TRUE** oder **version_2** setzen, indem Sie einen der folgenden Befehle ausführen:

```
odadmin set_allow_rconnect TRUE n
```

Dabei ist *n* die Objektdispatchernummer.

Weitere Informationen finden Sie im Handbuch *Tivoli Enterprise Console: Installationshandbuch*.

Einen speziellen Tivoli-Administrator für die Webschnittstelle definieren

Sie müssen ein spezielles Tivoli-Administratorenkonto erstellen, unter dem Sie die Webschnittstelle von Tivoli Remote Control verwenden können. Dieses Konto unterscheidet sich von Betriebssystem zu Betriebssystem.

- Unter UNIX, mit Ausnahme von HP-UX:

  Der Anmeldename des Administrators muss 'nobody' lauten.
- Unter Windows 2000 und HP-UX:

  Der Anmeldename des Administrators muss 'tmersrvd' lauten.

Wenn Sie diesen speziellen Administrator über den Tivoli-Desktop erstellen, führen Sie folgende Schritte aus:

1. Wählen Sie im Kontextmenü des Symbols **Administrator** die Option **Administrator erstellen** aus, um den Dialog 'Administrator erstellen' anzuzeigen.
2. Geben Sie in das Textfeld **Administratorname/Symbolbezeichnung** den Namen des Administrators ein.

3. Geben Sie in das Textfeld **Anmeldename des Benutzers** für UNIX-Maschinen (mit Ausnahme von HP-UX) 'nobody' und für Windows 2000- und HP-UX-Maschinen 'tmersrvd' ein.
4. Geben Sie in das Textfeld **Gruppenname** den Gruppennamen des Administrators ein (keine numerische Gruppen-ID).
5. Klicken Sie auf **Anmeldenamen festlegen**, um einen für den Tivoli-Server gültigen Anmeldenamen zu definieren wie beispielsweise: *nobody@Tivoli-Server*.
6. Klicken Sie auf **Erstellen & schließen**.

Weitere Informationen zum Erstellen und zur Verwendung des Tivoli-Administrators in Ihrer TMR-Umgebung finden Sie im Handbuch *Tivoli Management Framework: Benutzerhandbuch*.

Kapitel 5. Richtlinienbereiche für die Verwendung von Tivoli Remote Control konfigurieren

In diesem Kapitel wird erläutert, wie Richtlinienbereiche für die Verwendung von Tivoli Remote Control konfiguriert werden.

Vor der Verwendung von Tivoli Remote Control müssen folgende Tasks ausgeführt werden:

1. Die verwaltete Remote Control-Ressource zu einem Richtlinienbereich hinzufügen. Weitere Informationen finden Sie unter „Schritt 1: Die verwaltete Remote Control-Ressource zu einem Richtlinienbereich hinzufügen".
2. Ein Remote Control-Tool im Richtlinienbereich erstellen. Weitere Informationen finden Sie unter „Schritt 2: Ein Remote Control-Tool im Richtlinienbereich erstellen".
3. Den vorhandenen Berechtigungsklassen eines jeden Administrators die Berechtigungsklassen für Tivoli Remote Control hinzufügen. Weitere Informationen finden Sie unter „Schritt 3: Tivoli Remote Control-Berechtigungsklassen zuordnen" auf Seite 69.
4. Den Richtlinienbereichen, für die die Administratoren über Berechtigungsklassen in Tivoli Remote Control verfügen, Ziele zuordnen. Weitere Informationen finden Sie unter „Schritt 4: Richtlinienbereichen Ziele zuordnen" auf Seite 70.

Zu manchen Operationen finden Sie weitere Informationen in den Handbüchern *Tivoli Management Framework Benutzerhandbuch* und *Tivoli Management Framework Reference Manual*.

Schritt 1: Die verwaltete Remote Control-Ressource zu einem Richtlinienbereich hinzufügen

Jeder Richtlinienbereich verfügt über eine Liste der verwalteten Ressourcen. Um Tivoli Remote Control verwenden zu können, müssen Sie der Liste zunächst eine Remote Control-verwaltete Ressource hinzufügen. Sie können diese Task über den Tivoli-Desktop oder die Befehlszeile ausführen. Weitere Informationen zum Hinzufügen einer verwalteten Ressource zu einem Richtlinienbereich finden Sie in den Handbüchern von Tivoli Management Framework.

Schritt 2: Ein Remote Control-Tool im Richtlinienbereich erstellen

Nachdem Sie Remote Control als verwaltete Ressource festgelegt haben, müssen Sie ein Remote Control-Tool im Richtlinienbereich erstellen.

Führen Sie folgende Tasks aus, um ein Remote Control-Tool zu erstellen:

Schritt 2: Ein Remote Control-Tool erstellen

1. Wählen Sie in einem Richtlinienbereich **Erstellen → Remote Control** aus, um den Dialog 'Remote Control-Tool erstellen' anzuzeigen.

2. Geben Sie im Feld **Name/Symbolbezeichnung** einen eindeutigen Namen für das Remote Control-Tool an. Die folgenden Zeichen sind für den Namen nicht zulässig:
   Strichpunkt (;)
   Pipe-Zeichen (|)
   umgekehrter Apostroph (`)
   Dollarzeichen ($)
   Offene runde Klammer (( )
   Offene geschweifte Klammer ({)

   Enthält der Name Leerzeichen, muss er in Anführungszeichen (“ ”) gesetzt werden.
3. Um das Remote Control-Tool auf einem anderen verwalteten Knoten als dem Tivoli-Server zu erstellen, geben Sie den Namen des Knotens im Feld **Verwalteter Knoten** ein.

   Anmerkung: Der Tivoli Remote Control-Server muss auf dem von Ihnen angegebenen verwalteten Knoten installiert sein.
4. Klicken Sie auf die Schaltfläche **Erstellen & schließen**, um das Remote Control-Tool zu erstellen und zum Fenster 'Richtlinienbereich' zurückzukehren.

Alternativ dazu können Sie mit folgendem Befehl ein Remote Control-Tool in einem Richtlinienbereich erstellen:

```
wcreaterc <Kennung> <Position> <Richtlinienbereich>
```

Dabei gilt:

<Kennung> Gibt den Namen des Remote Control-Tools an, das erstellt werden soll.

<Position> Gibt den verwalteten Knoten an, auf dem das Remote Control-Tool erstellt werden soll.

Anmerkung: Der Tivoli Remote Control-Server muss auf dem von Ihnen angegebenen verwalteten Knoten installiert sein.

<Richtlinienbereich>
Gibt die Bezeichnung des Richtlinienbereichs an, in den das Remote Control-Tool eingefügt werden muss.

Weitere Informationen zum Befehl **wcreaterc** finden Sie im Anhang D, „Befehlszeilenschnittstelle”, auf Seite 149.

Anmerkung: Um ein Remote Control-Tool über den Tivoli-Desktop zu erstellen bzw. zu löschen, müssen Sie für den Richtlinienbereich, in dem Sie das Tool erstellen möchten, über die Berechtigungsklasse 'Admin' verfügen.

Schritt 3: Tivoli Remote Control-Berechtigungsklassen zuordnen

Nachdem Sie ein Remote Control-Tool erstellt haben, müssen Sie den Administratoren Tivoli Remote Control-Berechtigungsklassen zuordnen. Sie können Berechtigungsklassen nur dann zuordnen, wenn Sie über die erforderlichen Zugriffsberechtigungen verfügen.

Das Festlegen der Berechtigungsklassen auf der Ebene der Richtlinienbereiche ermöglicht Ihnen, die entsprechenden Tasks von Tivoli Remote Control innerhalb des angegebenen Richtlinienbereichs auszuführen. Diese Berechtigungen erstrecken sich nicht auf andere Richtlinienbereiche. Diese Berechtigungen gelten aber für alle untergeordneten Bereiche des Richtlinienbereichs, in dem die Tivoli Remote Control-Berechtigungsklassen definiert wurden.

Wenn der untergeordnete Bereich erstellt wurde, bevor Sie dem übergeordneten Richtlinienbereich neue Berechtigungen zugeordnet haben, werden diese Berechtigungen auf den untergeordneten Bereich nicht übertragen.

Das Festlegen der TMR-Berechtigungsklassen ermöglicht dem Administrator, die entsprechenden Tivoli Remote Control-Tasks in der gesamten Tivoli Management Region auszuführen.

Die Berechtigungsklassen für Tivoli Remote Control werden in dem Richtlinienbereich benötigt, in dem die Zielsysteme definiert sind. Zusätzlich zu diesen Berechtigungsklassen ist die Berechtigungsklasse **admin** in dem Bereich erforderlich, in dem die verwaltete Remote Control-Ressource definiert ist.

Eine Anleitung dazu, wie den Administratoren Berechtigungsklassen zugeordnet werden, finden Sie im *Tivoli Management Framework Benutzerhandbuch*.

In den folgenden zwei Tabellen sind die für Administratoren in Tivoli Remote Control verfügbaren Operationen und die dafür erforderlichen Berechtigungsklassen aufgeführt.

Operation	**Im Controller-Richtlinienbereich erforderliche Berechtigungsklasse**
Beliebige Tivoli Remote Control-Aktion verwenden	**admin**

Operation	**Im Ziel-Richtlinienbereich erforderliche Berechtigungsklasse**
Ein Ziel überwachen. Siehe Kapitel 9.	**remote_monitor**
Ein Ziel überwachen und steuern. Siehe Kapitel 9.	**remote_control**
Über die Befehlszeile **wrcmdpcr** Befehle auf einem Ziel ausführen. Siehe Kapitel 9.	**remote_probe**
Neustart eines Ziels ausführen. Siehe Kapitel 9.	**remote_reboot**

Schritt 3: Tivoli Remote Control-Berechtigungsklassen zuordnen

Operation	Im Ziel-Richtlinienbereich erforderliche Berechtigungsklasse
Textnachrichten mit einem Ziel austauschen. Siehe Kapitel 10.	**remote_chat**
Dateien vom Controller an ein Ziel senden. Siehe Kapitel 11, „Aktion 'Dateiübertragung' verwenden", auf Seite 113.	**remote_ft_send**
Dateien von einem Ziel empfangen. Siehe Kapitel 11.	**remote_ft_receive**

Schritt 4: Richtlinienbereichen Ziele zuordnen

Sie müssen den Richtlinienbereichen, für die die Administratoren über Berechtigungsklassen in Tivoli Remote Control verfügen, Ziele zuordnen.

Führen Sie folgende Schritte aus, um einem Richtlinienbereich ein Ziel zuzuordnen:

1. Stellen Sie sicher, dass der Richtlinienbereich, dem der Endpunkt zugeordnet werden soll, über die Endpunktressource in der Liste der verwalteten Ressourcenarten verfügt, die für diesen Richtlinienbereich gültig sind.
2. Verwenden Sie den Befehl **wmv** wie folgt:

   ```
   wmv @Endpoint:<Endpunktkennung> @PolicyRegion:<Richtlinienbereich>
   ```

   Dabei gilt:

<*Endpunktkennung*>	Gibt die zuzuordnende Endpunktbezeichnung an.
<*Richtlinienbereich*>	Gibt die Bezeichnung des Richtlinienbereichs an, in dem die Endpunktkennung zugeordnet sein muss.

3. Synchronisieren Sie das Tivoli-Gateway, an dem sich der Endpunkt anmeldet, mit den Befehlen **wep sync_gateways**.
4. Schließen Sie den Tivoli-Desktop, und starten Sie diesen erneut, um die Änderungen zu übernehmen.

Weitere Informationen zu diesen Befehlen finden Sie im Handbuch *Tivoli Management Framework Reference Manual*.

Kapitel 6. Standardeinstellungen des Remote Control-Tools ändern

Das Verhalten und die grafische Darstellung des Remote Control-Tools werden durch eine Standardrichtlinie gesteuert. Wenn Sie in einem Richtlinienbereich eine verwaltete Remote Control-Ressource erstellen, wird die Standardrichtlinie 'RemoteControl_PDO' automatisch der verwalteten Remote Control-Ressource zugeordnet und somit auch dem Remote Control-Tool dieses Richtlinienbereichs.

Dieses Kapitel enthält Folgendes:

- Die Schritte, die zum Ändern der Einstellungen des Remote Control-Tools erforderlich sind. Siehe „Remote Control-Standardrichtlinie ändern".
- Eine Beschreibung der Tivoli Remote Control-Richtlinienmethoden. Siehe „Tivoli Remote Control-Richtlinienmethoden" auf Seite 74.

Remote Control-Standardrichtlinie ändern

Um die Standardeinstellungen des Remote Control-Tools in einem Richtlinienbereich zu ändern, sollten Sie nicht die Standardrichtlinie 'RemoteControl_PDO' ändern, sondern eine neue Standardrichtlinie erstellen. Sie können auch für jede Instanz des Remote Control-Tools in den verschiedenen Richtlinienbereichen eine andere Remote Control-Standardrichtlinie erstellen.

Da eine Standardrichtlinie aus einer Reihe von Regeln besteht, den so genannten Richtlinienmethoden, müssen Sie die Werte einiger Methoden nach der Erstellung einer neuen Standardrichtlinie wie folgt ändern:

1. Erstellen Sie eine Kopie der Standardrichtlinie für die Remote Control-Ressource eines Richtlinienbereichs. Siehe „Schritt 1: Kopie der Remote Control-Standardrichtlinie erstellen".
2. Ändern Sie die Werte einiger Methoden dieser Standardrichtlinie. Siehe „Schritt 2: Inhalt einer Richtlinienmethode anpassen" auf Seite 72.
3. Ordnen Sie die neue Standardrichtlinie der verwalteten Remote Control-Ressource des Richtlinienbereichs zu, in dem sich das Remote Control-Tool befindet, das Sie anpassen möchten. Siehe „Schritt 3: Neue Remote Control-Standardrichtlinie zuordnen" auf Seite 73.

Schritt 1: Kopie der Remote Control-Standardrichtlinie erstellen

Führen Sie folgende Schritte aus, um eine Kopie der Remote Control-Standardrichtlinie zu erstellen:

1. Geben Sie folgende Syntax für den Befehl **wcrtpol** ein:

   ```
   wcrtpol -d RemoteControl RCPol RemoteControl_PDO
   ```

   Dabei gilt:

-d	Erstellt eine neue Standardrichtlinie.
RemoteControl	Gibt an, um welchen verwalteten Ressourcentyp es sich handelt.

RCPol	Gibt den Namen der neuen Remote Control-Standardrichtlinie an.
RemoteControl_PDO	Gibt den Namen der vorhandenen Remote Control-Standardrichtlinie an, von der die neue Richtlinie die ursprünglichen Methoden und Attribute übernimmt.

2. Überprüfen Sie, ob die Standardrichtlinie erstellt wurde, indem Sie die verfügbaren Standardrichtlinien für die verwaltete Remote Control-Ressource auflisten:

```
wlspol -d RemoteControl
Ausgabe:
RemoteControl_PDO
RCPol
...
```

3. Listen Sie die Richtlinienmethoden auf, die die Ressource steuern:

```
wlspolm -d RemoteControl
Ausgabe:
rc_def_command
rc_def_grace_time
rc_def_timeout_op
rc_def_polfilter_mode
...
```

Weitere Informationen zu den oben verwendeten Befehlen finden Sie in den Veröffentlichungen zu Tivoli Management Framework.

Schritt 2: Inhalt einer Richtlinienmethode anpassen

Führen Sie folgende Vorgänge aus, um den Wert einiger Methoden der Remote Control-Standardrichtlinie anzupassen:

1. Geben Sie folgenden Befehl ein, um den Hauptteil der angegebenen Richtlinienmethode, die einer Remote Control-Standardrichtlinie zugeordnet ist, zurückzugeben:

```
wgetpolm -d RemoteControl RCPol Methodenname > Ausgabedatei
```

Dabei gilt:

-d	Führt die angegebene Richtlinienmethode auf.
RemoteControl	Gibt an, um welchen verwalteten Ressourcentyp es sich handelt.
RCPol	Gibt den Namen einer Remote Control-Standardrichtlinie an.
Methodenname	Gibt den Namen der Richtlinienmethode an, deren Hauptteil ersetzt werden soll.
Ausgabedatei	Gibt den Namen einer Ausgabedatei an.

2. Verwenden Sie einen Zeileneditor, um die Ausgabedatei zu ändern.
3. Geben Sie folgenden Befehl ein, um den Hauptteil der angegebenen Richtlinienmethode zu ersetzen:

```
wputpolm -d RemoteControl RCPol Methodenname < Ausgabedatei
```

Die Argumente sind dieselben wie für den Befehl **wgetpolm** oben in Schritt 1.

Schritt 3: Neue Remote Control-Standardrichtlinie zuordnen

Sie können die neue Standardrichtlinie der verwalteten Remote Control-Ressource des Richtlinienbereichs über den Tivoli-Desktop oder über die Befehlszeile zuordnen.

Über den Tivoli-Desktop

1. Öffnen Sie den Richtlinienbereich, der das Remote Control-Tool enthält, dem Sie die neue Standardrichtlinie 'RCPol' zuordnen möchten.
2. Wählen Sie **Merkmale → Richtlinien für verwaltete Ressourcen** aus.
3. Wählen Sie im Dialog 'Richtlinien für verwaltete Ressourcen' aus der Liste **Verwaltete Ressourcen** 'RemoteControl' aus.
4. Wählen Sie aus der Dropdown-Liste **Standardwertegruppe** 'RCPol' aus.
5. Klicken Sie auf **Festlegen und schließen**.

Über die Befehlszeile

Geben Sie folgenden Befehl ein:

```
wsetpr -d RCPol RemoteControl @PolicyRegion:rc-region
```

Dabei gilt:

-d RCPol
Gibt 'RCPol' als neue Standardrichtlinie an.

RemoteControl
Gibt 'RemoteControl' als verwaltete Ressource an, für die die neue Standardrichtlinie definiert wird.

@PolicyRegion:rc-region
Gibt 'rc-region' als Richtlinienbereich an, für den die neue Standardrichtlinie zugeordnet werden soll.

Zusammenfassung der Standardrichtlinienmethoden

Mit Hilfe der folgenden Richtlinienmethoden der Standardrichtlinie, die der verwalteten Remote Control-Ressource zugeordnet ist, können Sie die Standardwerte des Remote Control-Tools ändern.

Richtlinienmethode	Funktion	Seite
rc_def_alt_t	Bestimmt die Verwendung von <Alt><T> auf dem Ziel	75
rc_def_backgrnd	Bestimmt die Verfügbarkeit von Hintergrund und Bildschirmschoner auf dem Ziel	75
rc_def_color	Bestimmt die Anzahl der Farben, die beim Anzeigen des Zielbildschirms auf dem Controller verwendet werden	75
rc_def_command	Bestimmt die für Administratoren verfügbaren Aktionen	76
rc_def_comp	Bestimmt die Datenkomprimierung	76
rc_def_define	Bestimmt die Kriterien für die Anzeige von Zielen	77
rc_def_encryption	Bestimmt die Datenverschlüsselung	77
rc_def_ftmode	Bestimmt die verfügbaren Arten von Dateiübertragungsaktionen	78

Remote Control-Standardrichtlinie ändern

Richtlinienmethode	Funktion	Seite
rc_def_grace_time	Bestimmt die Zeitdauer, in der ein Benutzer auf eine Aktionsanforderung reagieren kann	78
rc_def_gw	Bestimmt, ob ein Remote Control-Gateway verwendet wird	79
rc_def_inactivity	Bestimmt die Zeitdauer, in der die Sitzung ohne Benutzeraktion aktiv bleibt. Bei Überschreitung des Zeitlimits wird die Sitzung geschlossen.	79
rc_def_initstate	Bestimmt den Anfangsstatus der Sitzung. Nur wirksam, wenn für 'rc_def_rcmode' der Wert **control** festgelegt ist.	80
rc_def_optimize	Bestimmt die Leistungsoptimierung bei langsamen Verbindungen	80
rc_def_polfilter_mode	Bestimmt, ob Ziele nur für einen angegebenen Bereich angezeigt werden	80
rc_def_ports	Bestimmt die Anschlüsse, die für die Kommunikation zwischen Controller und Ziel verwendet werden	81
rc_def_proxy	Bestimmt, ob Remote Control-Proxys verwendet werden	82
rc_def_rate	Bestimmt die Bildwiederholfrequenz der Controlleranzeige	83
rc_def_rcmode	Bestimmt die möglichen Aktivitäten für eine Remote Control-Aktion	83
rc_def_targets	Bestimmt, ob ein Ziel der Zielmaschinenliste hinzugefügt wird	84
rc_def_timeout_op	Bestimmt, ob eine Sitzung nach Ablauf der Reaktionszeit beendet wird	84
rc_def_uncheckedlist	Bestimmt die anzuzeigenden Ziele, wenn für 'rc_def_define' der Wert **UncheckedList** festgelegt ist	84

Tivoli Remote Control-Richtlinienmethoden

Die folgenden Richtlinienmethoden gehören zu der Standardrichtlinie, die der verwalteten Ressource 'RemoteControl' zugeordnet ist. Mit diesen Richtlinienmethoden können Sie die Standardeinstellungen des Remote Control-Tools in einem Richtlinienbereich steuern. Bei der Angabe der Werte in den Richtlinienmethoden müssen Sie die Groß-/Kleinschreibung beachten.

Die Richtlinienmethoden werden mit Hilfe der Shell-Scriptbindung implementiert. Von diesen Methoden wird eine Zeichenfolge zurückgegeben, die in die Standardausgabe geschrieben wird. Für die Methoden ist ein Standardwert festgelegt, den Sie wie in „Schritt 2: Inhalt einer Richtlinienmethode anpassen" auf Seite 72 beschrieben ändern können. Diese Methoden können je nach Richtlinienbereich unterschiedlich sein. In einem Richtlinienbereich kann eine bestimmte Gruppe von Standardrichtlinienmethoden gelten, und einem anderen Richtlinienbereich können auch andere Richtlinienmethoden zugeordnet sein.

rc_def_alt_t

Bestimmt, ob der Benutzer des Zielrechners die Tastenkombination <Alt><T> zum Ändern des Status während einer Remote Control-Sitzung verwenden kann. Folgende Status sind möglich: *Aktivieren*, *Überwachen*, *Suspendieren* und *Beenden*.

Gültige Werte:

ENABLED
Die Tastenkombination <Alt><T> ist aktiviert.

DISABLED
Die Tastenkombination <Alt><T> ist inaktiviert.

DEPEND-ON-TARGET
Die Tastenkombination <Alt><T> ist aktiviert und der Benutzer des Zielrechners kann den Sitzungsstatus in 'Aktivieren' ändern, auch wenn der Benutzer des Controllers in dem Bereich nur über die Berechtigungsklasse 'remote_monitor' verfügt oder für 'rc_def_mode' 'Überwachen' festgelegt ist.

Standardwert: **DISABLED**

Wenn der Wert das Suffix **-locked** hat, kann er im Dialog 'Einstellungen editieren' nicht geändert werden.

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "DISABLED"
exit 0
```

rc_def_backgrnd

Bestimmt, ob der Bildschirmhintergrund des Zielrechners inaktiviert werden soll.

Gültige Werte:

On Der Hintergrund und der Bildschirmschoner werden inaktiviert.

Off Der Hintergrund und der Bildschirmschoner werden nicht inaktiviert.

Standardwert: **On**

Wenn der Wert das Suffix **-locked** hat, kann er im Dialog 'Einstellungen editieren' nicht geändert werden.

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "On"
exit 0
```

rc_def_color

Bestimmt die Anzahl der Farben, die beim Anzeigen des Zielbildschirms auf dem Controller verwendet werden

Gültige Werte:

0 Anzahl der auf der Zielanzeige verwendeten Farben

4 16 Farben

8 256 Farben

Standardwert: **8**

Wenn der Wert das Suffix **-locked** hat, kann er im Dialog 'Einstellungen editieren' nicht geändert werden.

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "8"
exit 0
```

rc_def_command

Bestimmt, ob eine Aktion verfügbar ist.

Gültige Werte:

Jede Kombination der folgenden Kennungen, getrennt durch ein Semikolon (;).

rc Remote Control

reboot Neustart

filexfer Dateiübertragung

Chat Chat

Standardwert: **reboot;chat;filexfer;rc;**

Die zuletzt angegebene Kennung wird als Standardaktion verwendet.

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "reboot;chat;filexfer;rc"
exit 0
```

rc_def_comp

Bestimmt, ob die an den Controller übertragenen Daten komprimiert werden. Wenn die verwaltete Remote Control-Ressource so konfiguriert ist, dass sie ein Tivoli Remote Control-Gateway verwendet, wird diese Methode ignoriert, und die Daten werden immer komprimiert.

Gültige Werte:

On Die Daten werden komprimiert.

Off Die Daten werden nicht komprimiert.

Standardwert: **On**

Wenn der Wert das Suffix **-locked** hat, kann er im Dialog 'Einstellungen editieren' nicht geändert werden.

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "On"
exit 0
```

rc_def_define

Legt den Aufbau und die Anzeige der Liste für die Ziele fest.

Gültige Werte:

DefinableTargetList	Auflistung nach Zielkennung gemäß **rc_def_targets**
FilteredList	Auflistung nach Richtlinienbereich gemäß **rc_def_polfilter_mode** und nach Kennung gemäß **rc_def_targets**
UncheckedList	Auflistung gemäß **rc_def_uncheckedlist**. Siehe Seite 84.

Standardwert: **DefinableTargetList**

Wenn der Wert **DefinableTargetList** oder **FilteredList** lautet, wird ein Ziel nur aufgelistet, wenn es zu der Richtlinienmethode **rc_def_targets** gehört. Siehe Seite 84.

Wenn der Wert **DefinableTargetList** lautet, kann die Zielmaschinenliste im Dialog 'Zielmaschinenliste definieren' zurückgesetzt werden. Siehe „Vorhandene Zielmaschinenliste über einen Dialog ändern" auf Seite 89. Die editierte Liste wird zur späteren Verwendung in der Richtlinienmethode **rc_def_targets** gespeichert.

Wenn der Wert **DefinableTargetList** das Suffix **-locked** hat, kann die Zielmaschinenliste im Dialog 'Zielmaschinenliste definieren' nicht geändert werden.

Wenn Sie den Befehl **wrc** verwenden und die Zielmaschinen gemäß den Richtlinienmethoden filtern möchten, müssen Sie das Suffix **-apply2cli** zum angegebenen Wert für 'rc_def_define' hinzufügen. Dieses Suffix ist sinnvoll, wenn Sie für 'DefinableTargetList' 'locked' festlegen oder wenn Sie bei Verwendung von 'FilteredList' für 'rc_def_polfilter_mode' 'locked' angeben.

Anmerkung: Die Suffixe **-locked** und **-apply2cli** können wie folgt zusammen angegeben werden:

```
#DefinableTargetList-locked-apply2cli
#DefinableTargetList-apply2cli-locked
```

Beispiel des Shell-Scripts:

```
#!/bin/sh

# This script filters targets according to rc_def_uncheckedlist.
# The filter does not work with the wrc command.
echo "UncheckedList"
exit 0
```

Beispiel des Shell-Scripts:

```
#!/bin/sh
# This script filters targets according to rc_def_uncheckedlist.
# The filter also works with the wrc command.
echo "UncheckedList-apply2cli"
exit 0
```

rc_def_encryption

Bestimmt, ob die bei folgenden Sitzungen übertragenen Daten verschlüsselt werden:

- Remote Control-Sitzung zwischen Windows NT-, Windows 2000-, Windows XP- oder Windows 98 Second Edition-Controllern und Windows NT-, Windows 2000- oder Windows XP-Zielrechnern.
- Eine Dateiübertragungssitzung zwischen Controllern und Zielrechnern mit jedem anderen unterstützten Betriebssystem.

Gültige Werte:

No Die Daten werden nicht verschlüsselt.

Yes Alle Daten außer den Daten, die während einer Chat-Sitzung ausgetauscht werden, werden verschlüsselt.

Standardwert: **No**

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "No"
exit 0
```

rc_def_ftmode

Bestimmt, welche Dateiübertragungsvorgänge Sie ausführen können. Dies hängt von Ihrer Berechtigungsklasse für Tivoli Remote Control ab.

Gültige Werte:

send Wenn Sie über die Berechtigungsklasse **remote_ft_send** verfügen, können Sie Dateien senden.

receive Wenn Sie über die Berechtigungsklasse **remote_ft_receive** verfügen, können Sie Dateien empfangen.

both Wenn Sie über die Berechtigungsklassen **remote_ft_send** und **remote_ft_receive** verfügen, können Sie Dateien senden oder empfangen.

Standardwert: **both**

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "both"
exit 0
```

rc_def_grace_time

Bestimmt, wie viele Sekunden der Zielrechnerbenutzer Zeit zum Reagieren hat, bevor eine Aktion gestartet oder wegen Zeitlimitüberschreitung nicht gestartet wird.

Gültige Werte:

0 0 Sekunden
5 5 Sekunden
10 10 Sekunden
15 15 Sekunden
30 30 Sekunden
60 1 Minute
120 2 Minuten
240 4 Minuten
480 8 Minuten

960 16 Minuten

Standardwert: **5**

Wenn der Wert **0** festgelegt ist, wird am Bildschirm des Zielrechners kein Dialogfenster zur Bestätigung angezeigt.

Wenn der Wert das Suffix **-locked** hat, kann er im Dialog 'Einstellungen editieren' nicht geändert werden.

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "5"
exit 0
```

rc_def_gw

Bestimmt, ob das Remote Control-Gateway verwendet wird.

Gültige Werte:

NO Das Remote Control-Gateway wird nicht verwendet.

YES <*VerwKnoten_Kennung***> <***Gateway-Port***> <***MaxSitzungen***> IP:<***IP-Port***>**
Das angegebene Remote Control-Gateway wird verwendet. Dabei gilt:

<*VerwKnoten_Kennung*> ist der Name des verwalteten Knotens, der als Remote Control-Gateway eingesetzt wird.

<*Gateway-Port*> ist der TCP/IP-Port, der vom Remote Control-Gateway zum Abruf von Verbindungsanforderungen von Controllern verwendet wird.

< *MaxSitzungen*> ist die Anzahl an Tivoli Remote Control-Sitzungen zwischen einem Controller und einem Zielrechner, die ein Remote Control-Gateway auf einem eingehenden Port verarbeiten kann. Der Maximalwert beträgt 64.

<*IP-Port*> ist der lokale TCP/IP-Port, der vom Remote Control-Gateway zur Kommunikation mit TCP/IP-Zielrechnern verwendet wird. Wenn der Wert **0** lautet, verwendet das Remote Control-Gateway einen vom Kommunikations-Stack generierten Port.

Standardwert: **NO**

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "YES enigm2 35000 16 IP:0"
exit 0
```

Anmerkung: Wenn Sie die Remote Control-Proxys verwenden, wird die durch die Richtlinienmethode 'rc_def_gw policy' festgelegte Konfiguration ignoriert.

rc_def_inactivity

Bestimmt, wie viele Minuten eine Sitzung ohne Tastatur- oder Mausaktivität aktiv bleibt.

Gültige Werte:

0 Für die Sitzung gilt kein Zeitlimit.

<*ganze_Zahl*> Für die Sitzung gilt ein Zeitlimit von <*ganze_Zahl*> Minuten.

Standardwert: **0**

Wenn der Wert das Suffix **-locked** hat, kann er im Dialog 'Einstellungen editieren' nicht geändert werden.

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "0"
exit 0
```

rc_def_initstate

Bestimmt den Anfangsstatus einer Remote Control-Aktion. Der Wert hat nur dann Auswirkungen, wenn für **rc_def_rcmode** der Wert **control** festgelegt ist. Siehe Seite 83.

Gültige Werte:

monitor Die Aktion wird im überwachten Status gestartet.

active Die Aktion wird im aktiven Status gestartet.

Standardwert: **Monitor**

Wenn der Wert das Suffix **-locked** hat, kann er im Dialog 'Einstellungen editieren' nicht geändert werden.

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "monitor"
exit 0
```

rc_def_optimize

Optimiert die Leistung der Remote Control-Sitzung, wenn Sie eine langsame Verbindung auf Windows NT-, Windows 2000- oder Windows XP-Zielrechnern verwenden. Weitere Informationen zur Leistung finden Sie unter „Leistung steigern" auf Seite 133.

Gültige Werte:

ENABLED Die Leistungsoptimierung ist aktiviert.

DISABLED Die Leistungsoptimierung ist inaktiviert.

Standardwert: **DISABLED**

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "DISABLED"
exit 0
```

rc_def_polfilter_mode

Bestimmt, ob Zielrechner eines bestimmten Richtlinienbereichs angezeigt werden.

Diese Methode hat nur dann Auswirkungen, wenn für **rc_def_define** der Wert **FilteredList** festgelegt ist. Siehe Seite 77.

Gültige Werte:

region Es werden die Ziele des Richtlinienbereichs angezeigt, der im Zielmaschinenlistendialog ausgewählt wurde.

byregion Es werden nur die Ziele des Richtlinienbereichs angezeigt, zu dem das Remote Control-Tool gehört.

all Es werden alle Ziele angezeigt.

Standardwert: **byregion**

Wenn der Wert das Suffix **-locked** hat, kann er im Dialog 'Einstellungen editieren' nicht geändert werden.

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "byregion"
exit 0
```

rc_def_ports

Legt die Anschlüsse fest, die Controller und Zielrechner zur Kommunikation verwenden.

Gültige Werte:

```
rc TIP:<Ziel-TCP/IP-Port>
   CIP:<Controller-TCP/IP-Port><\n>
filexfer TIP:<Ziel-TCP/IP-Port>
   CIP:<Controller-TCP/IP-Port><\n>
chat TIP:<Ziel-TCP/IP-Port>
   CIP:<Controller-TCP/IP-Port><\n>
```

Dabei gilt:

rc Legt die Ports für die Remote Control-Aktion fest.

filexfer Legt die Ports für die Dateiübertragungsaktion fest.

Chat Legt die Ports für die Chat-Aktion fest.

<*Ziel-TCP/IP-Port***>** Der Ziel-TCP/IP-Port, der für die Verbindung empfangsbereit ist. Gültige Werte:

- **<***Port***>** Portnummer
- **0** Standardport (2501 für Remote Control, 2502 für Dateiübertragung, 2503 für Chat)

<*Controller-TCP/IP-Port*> Der Controller-TCP/IP-Port, der zum Starten der Verbindung verwendet wird. Gültige Werte:

- <*Port*> Portnummer
- **0** Der Port wird vom Kommunikations-Stack zugeordnet.

<*n*> Bezeichnet das Zeilenvorschubzeichen.

Standardwerte:

```
rc TIP:0 CIP:0<\n>
filexfer TIP:0 CIP:0<\n>
chat TIP:0 CIP:0<\n>
```

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "rc TIP:0 CIP:0"
echo "filexfer TIP:0 CIP:0"
echo "chat TIP:0 CIP:0"
exit 0
```

rc_def_proxy

Bestimmt, ob Remote Control-Proxys verwendet werden. Wenn Sie Remote Control-Proxys verwenden, bestimmt 'rc_def_proxy defines', wie der Controller die Remote Control-Proxys zum Starten einer Sitzung mit einem Zielrechner über eine Firewall verwendet.

Gültige Werte:

NO Die Remote Control-Proxys werden nicht verwendet.

YES <*Konfigurationstyp*> <*RC-Proxy-IP-Adresse*> <*RC-Proxy-Port*>
Die Remote Control-Proxys werden verwendet. Dabei gilt:

<*Konfigurationstyp*>
Gibt folgende Szenarios an:

auto Der Controller und Remote Control-Proxys suchen mit Hilfe der von IBM Tivoli Firewall Security Toolbox gespeicherten Informationen die Route zum Zielrechner.

manual
Die Remote Control-Proxys werden im Standalone-Modus ausgeführt. Der Controller verwendet die Netzwerkadresse, die Sie in dieser Methode angeben, um die Maschine zu erreichen, auf der der Zielproxy ausgeführt wird.

<*RC-Proxy-IP-Adresse*>
Gibt die Maschine an, auf der der Zielproxy ausgeführt wird. Sie dürfen diesen Parameter nur mit dem Konfigurationstyp **manual** verwenden.

<*RC-Proxy-Port*>
Gibt den Port an, über den der Zielproxy mit dem Controller oder dem Controller-Proxy kommuniziert.

Standardwert: **NO**

Beispiele für Shell-Scripts:

- ```
  #!/bin/sh
  echo "YES auto 3501"
  exit 0
  ```
- ```
  #!/bin/sh
  echo "YES manual 192.168.100.50 3501"
  exit 0
  ```

Anmerkung: Wenn Sie die Remote Control-Proxys verwenden, wird die durch die Richtlinienmethode 'rc_def_gw policy' festgelegte Konfiguration ignoriert.

rc_def_rate

Legt fest, wie viele Millisekunden mindestens zwischen zwei aufeinanderfolgenden Bildschirmaktualisierungen liegen müssen, die vom Zielrechner an den Controller gesendet werden.

Gültige Werte:

<*ganze_Zahl*> Ganze Zahlen, die größer oder gleich **50** sind. Wenn Sie Remote Control in einer LAN-Umgebung verwenden, ist der empfohlene Wert **50**. Wenn Sie Remote Control mit Modemdatenübertragung verwenden, ist der empfohlene Wert **500**. Der empfohlene Maximalwert ist **4000**.

Standardwert: **50**

Wenn der Wert das Suffix **-locked** hat, kann er im Dialog 'Einstellungen editieren' nicht geändert werden.

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "50"
exit 0
```

rc_def_rcmode

Bestimmt die für eine Remote Control-Sitzung verfügbaren Aktionen.

Gültige Werte:

control Wenn der Administrator auf dem Zielrechner über die Berechtigungsklasse **remote_control** verfügt, kann eine aktive Sitzung gestartet werden. Der Anfangsstatus wird durch **rc_def_initstate** festgelegt. Siehe Seite 80. Der Administrator kann den Status in **monitor** ändern.

Wenn der Administrator auf dem Ziel über die Berechtigungsklasse **remote_monitor** verfügt, kann nur eine Überwachungssitzung gestartet werden. Der Administrator kann den Status nicht in **control** ändern.

monitor Wenn der Administrator über eine oder beide der Berechtigungsklassen **remote_monitor** und **remote_control** verfügt, wird eine Überwachungssitzung gestartet. Der Administrator kann den Status nicht in **control** ändern.

Standardwert: **control**

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "control"
exit 0
```

rc_def_targets

Definiert eine Liste mit Zielkennungen, die verwendet wird, wenn für **rc_def_define** der Wert **DefinableTargetList** oder **FilteredList** angegeben ist. Siehe Seite 77.

Gültige Werte:

default-list Es werden alle Ziele angezeigt.

<*Zielkennung*> **[{**<*n*> <*Zielkennung*>**}]**
Die Ziele auf der Liste werden angezeigt. Dabei gilt:

<*Zielkennung*> Gibt den Namen eines Endpunkts an.

<*n*> Bezeichnet das Zeilenvorschubzeichen.

Standardwert: **default-list**

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "default-list"
exit 0
```

rc_def_timeout_op

Bestimmt, ob eine Sitzung gestartet wird, falls der Benutzer des Zielrechners nicht innerhalb der festgelegten Reaktionszeit antwortet.

Gültige Werte:

ENABLED Bei einer Zeitlimitüberschreitung wird die Sitzung gestartet.

DISABLED Bei einer Zeitlimitüberschreitung wird die Sitzung nicht gestartet.

Standardwert: **DISABLED**

Wenn der Wert das Suffix **-locked** hat, kann er im Dialog 'Einstellungen editieren' nicht geändert werden.

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo "DISABLED"
exit 0
```

rc_def_uncheckedlist

Bestimmt den Inhalt der Zielmaschinenliste, wenn für die Methode **rc_def_define** der Wert **UncheckedList** angegeben ist. Siehe Seite 77.

Gültige Werte:

<*Endpunktkennung*>[{<*n*>
<*Endpunktkennung*>}]

Dabei gilt:

<*Endpunktkennung*>
Gibt den Namen eines Endpunkts an.

<*n*>
Bezeichnet das Zeilenvorschubzeichen.

Standardwert:

```
wgetallinst Endpoint
```

Beispiel des Shell-Scripts:

```
#!/bin/sh
echo target1_ep
echo target2_ep
echo target3_ep
exit 0
```

Tivoli Remote Control-Richtlinienmethoden<

Kapitel 7. Tivoli Remote Control-Schnittstelle anpassen

In diesem Kapitel wird beschrieben, wie Sie Folgendes anpassen können:

- Den Dialog mit den Zielmaschinen und den Dialog 'Einstellungen editieren', die dem Remote Control-Tool eines Richtlinienbereichs zugeordnet sind. Insbesondere wird erläutert, welche Richtlinienmethoden sich auf die Einstellungen der grafischen Benutzerschnittstelle vonTivoli Remote Control oder der Webschnittstelle auswirken.

  Anmerkung: Wenn Sie die Einstellungen über die Schnittstelle anpassen, gelten folgende Einschränkungen:
  - Sie können nur die angezeigten Einstellungswerte ändern, die nicht durch eine Richtlinienmethode gesperrt wurden.
  - Durch die neuen Werte werden nur die aktuellen Einstellungen geändert, nicht die Standardeinstellungen, die der Standardrichtlinie entnommen werden. Die einzige Ausnahme stellt die Zielmaschinenliste dar: Wenn sie gespeichert wird, ist sie der Standardwert für die Methode **rc_def_targets**. Siehe „rc_def_targets" auf Seite 84.
- Die Tivoli Remote Control-Webseite.

Zielmaschinenliste anpassen

Wenn Sie das Remote Control-Tool starten, wird ein Dialog angezeigt, der eine Liste mit Zielmaschinen enthält. Um verschiedene Zielmaschinenlisten zu generieren, müssen Sie den Wert der Richtlinienmethode **rc_def_define** in einen der folgenden Werte ändern:

DefinableTargetList — Zeigt die Liste der Zielmaschinenkennungen an, die in 'rc_def_targets' definiert sind. Siehe „Für 'rc_def_define' den Wert 'DefinableTargetList' festlegen" auf Seite 88.

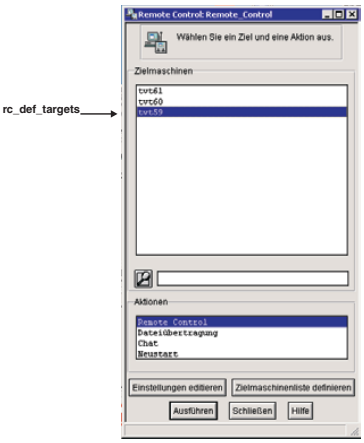
FilteredList — Zeigt die Liste der Zielmaschinenkennungen an, die in 'rc_def_targets' aufgeführt sind und zu einem Richtlinienbereich gehören, der in 'rc_def_polfilter_mode' definiert ist. Siehe „Für 'rc_def_define' den Wert 'FilteredList' festlegen" auf Seite 88.

UncheckedList — Zeigt die Liste der Zielmaschinenkennungen an, die in 'rc_def_uncheckedlist' definiert sind. Die Zielmaschinenkennungen werden nicht überprüft, bevor sie aufgelistet werden. Nach der Auswahl der Zielmaschine wird eine Überprüfung durchgeführt. Siehe „Für 'rc_def_define' den Wert 'UncheckedList' festlegen" auf Seite 89.

Je nachdem, welcher Wert für 'rc_def_define' ausgewählt wird, werden folgende Dialoge angezeigt.

Für 'rc_def_define' den Wert 'DefinableTargetList' festlegen

Wenn Sie für die Richtlinienmethode **rc_def_define** den Wert **DefinableTargetList** angeben, wird der Dialog 'Remote Control' mit einer Zielmaschinenliste wie in der folgenden Abbildung angezeigt:



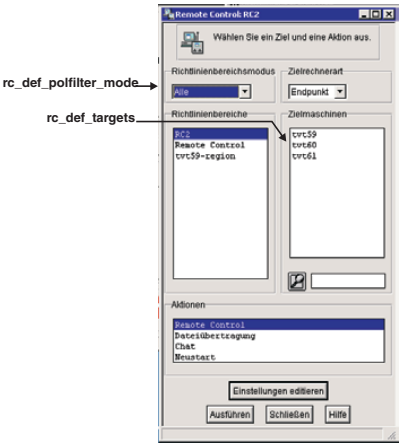
In diesem Dialog sind die Zielmaschinen aufgeführt, die in der Richtlinienmethode **rc_def_targets** definiert sind. Ausführliche Informationen finden Sie auf Seite 84.

Über die Schaltfläche **Zielmaschinenliste definieren** können Sie die Zielmaschinenliste ändern.

Anmerkung: Diese Schaltfläche ist inaktiviert, wenn für die Richtlinienmethode **rc_def_define** der Wert **DefinableTargetList-locked** angegeben ist.

Für 'rc_def_define' den Wert 'FilteredList' festlegen

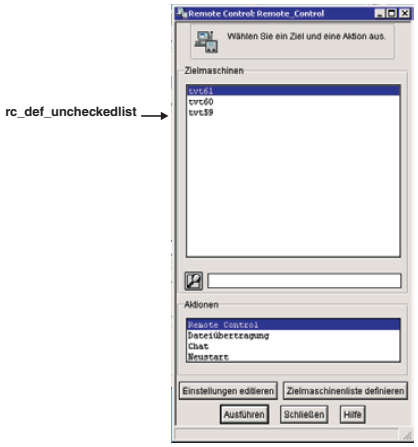
Wenn Sie für die Richtlinienmethode **rc_def_define** den Wert **FilteredList** angeben, wird der Dialog 'Remote Control' mit Richtlinienbereichen und einer Zielmaschinenliste wie in der folgenden Abbildung angezeigt:



In diesem Dialog sind die Zielmaschinen aufgeführt, die in der Richtlinienmethode **rc_def_targets** definiert sind und die zu einem Richtlinienbereich oder zu allen Richtlinienbereichen gehören, die in der Richtlinienmethode **rc_def_polfilter_mode** definiert sind.

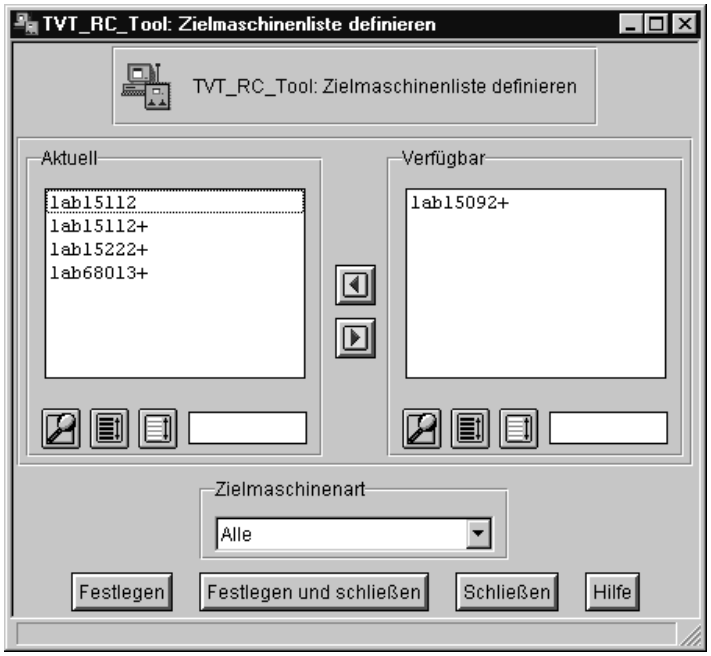
Für 'rc_def_define' den Wert 'UncheckedList' festlegen

Wenn Sie für die Richtlinienmethode **rc_def_define** den Wert **UncheckedList** angeben, wird der Dialog 'Remote Control' mit einer Zielmaschinenliste wie in der folgenden Abbildung angezeigt:



Vorhandene Zielmaschinenliste über einen Dialog ändern

Wenn Sie in einem Remote Control-Dialog auf **Zielmaschinenliste definieren** klicken, wird der Dialog 'Zielmaschinenliste definieren' angezeigt.



Die bereits ausgewählten Zielrechner werden in der Liste **Aktuell** aufgeführt. Die verfügbaren Zielrechner werden in der Liste **Verfügbar** angezeigt. Um ein Ziel zwischen den Listen zu verschieben, wählen Sie es aus und klicken Sie entsprechend auf den Links- oder Rechtspfeil. Wenn Sie die in der Liste angezeigten Zielmaschinenarten eingrenzen möchten, wählen Sie die gewünschte Art in der Dropdown-Liste 'Zielrechnerart' aus.

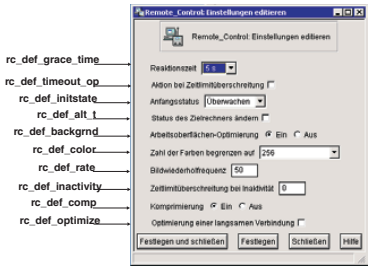
Vorhandene Zielmaschinenliste über einen Dialog ändern

Änderungen der Liste 'Aktuell' werden in der Shell-Datei, die der Richtlinienmethode **rc_def_targets** zugeordnet ist, gespeichert. Klicken Sie auf **Festlegen** oder **Festlegen und schließen**, um die Änderungen zu übernehmen. Im daraufhin angezeigten Dialogfeld werden Sie zum Bestätigen der Änderungen aufgefordert. Weitere Informationen finden Sie unter „rc_def_targets" auf Seite 84.

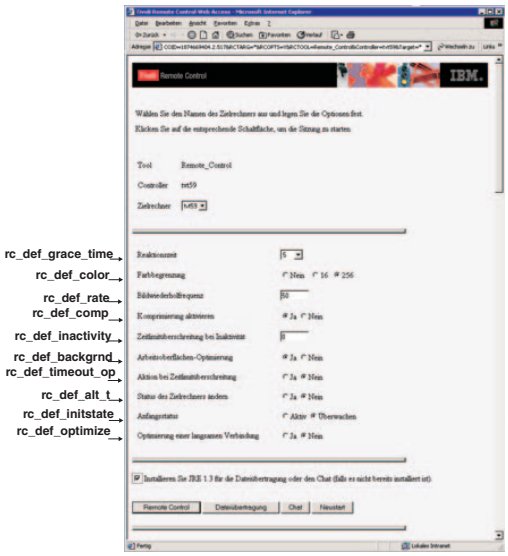
Sitzungseinstellungen anpassen

Sie können die Sitzungseinstellungen über die Tivoli Remote Control-Schnittstelle oder über die Richtlinienmethoden ändern. Wenn Sie die Schnittstelle verwenden, werden nur die aktuellen Einstellungen geändert, nicht die Standardeinstellungen, die der Standardrichtlinie entnommen werden. In den folgenden Abbildungen wird die Beziehung zwischen den Sitzungseinstellungen und den Richtlinienmethoden, die sich auf diese auswirken, verdeutlicht:

- **Grafische Benutzerschnittstelle:** Wenn Sie in einem Remote Control-Dialog auf **Einstellungen editieren** klicken, wird der Dialog 'Einstellungen editieren' angezeigt.



- **Webschnittstelle:** Wenn Sie die Webschnittstelle verwenden, werden vor dem Start einer Sitzung dieselben Einstellungen auf der folgenden Webseite angezeigt:



Weitere Informationen zu den Einstellungen finden Sie in den Beschreibungen der jeweiligen Richtlinienmethoden unter „Tivoli Remote Control-Richtlinienmethoden" auf Seite 74.

Tivoli Remote Control-Webseite anpassen

Die Standardseite (default.html) enthält einen Link zur Anwendung Tivoli Remote Control, bei dem das Script 'pcremoteaccess.cgi' verwendet wird.

Sie können die Webseite für Tivoli Remote Control ändern, indem Sie die Datei 'default.html' editieren. Standardmäßig enthält diese Datei einen Link, der das Script 'pcremoteaccess.cgi' verwendet. Um die Werte, die Sie in der Tivoli Remote Control-Webschnittstelle anzeigen möchten, zu filtern, können Sie diesem Script unter Verwendung der folgenden Syntax vier Parameter (0 bis 3) hinzufügen. (Alternativ dazu können Sie die gewünschten Parameter auch in der Befehlszeile des Browsers eingeben.)

```
pcremoteaccess.cgi?RCTOOL=x&RCCTRL=x&RCTARG=x&RCACTN=x
```

Dabei gilt:

RCTOOL Name des Tivoli Remote Control-Tools

RCCTRL Controllername

RCTARG Zielmaschinenname. Wenn ein Name angegeben wird, wird dieser standardmäßig einem Endpunktziel zugeordnet. Wenn Sie verschiedene Arten von Zielen definieren möchten, müssen Sie folgende Syntax verwenden:

```
<Zielmaschinenname>
```

RCACTN Tivoli Remote Control-Aktion. Folgende Werte sind gültig:

```
[rc|reboot|filexfer|chat]
```

Anmerkung: Nachdem die Änderungen vorgenommen wurden, muss die Standardseite (default.html) neu geladen werden. Dazu müssen Sie die Befehle **wstophttpd** und **wstarthttpd** in der Befehlszeile von Tivoli Management Framework ausführen.

Wenn Sie Ihre eigene Webseite verwenden möchten, rufen Sie das Script **startsession.cgi** mit folgender Syntax auf:

```
startsession.cgi?RemoteControl=x&Controller=x&Target=x&Action=x
[&G=x&P=x&D=x&B=x&C=x&T=x&Z=x&R=x&I=x&S=x]
```

Dabei gilt:

RemoteControl Name des Tivoli Remote Control-Tools

Controller Controllername. Verwenden Sie zum Definieren des Controllers folgende Syntax:

```
<Controllername>
```

Target Zielmaschinenname. Verwenden Sie zum Definieren der Zielmaschine folgende Syntax:

```
<Zielmaschinenname>
```

Action Tivoli Remote Control-Aktion. Folgende Werte sind gültig:

```
[rc|reboot|filexfer|chat]
```

Erläuterungen zu den sonstigen Optionen finden Sie unter „wrc" auf Seite 154.

Tivoli Remote Control-Webseite anpassen

Kapitel 8. Tivoli Remote Control starten

In diesem Kapitel wird beschrieben, wie eine Sitzung in Tivoli Remote Control gestartet wird. Informationen zur Verwendung der einzelnen Aktionen in Tivoli Remote Control finden Sie in den Kapiteln 4 bis 7.

Eine Tivoli Remote Control-Aktion starten

Tivoli Remote Control-Aktionen können über den Tivoli-Desktop, die Befehlszeile (siehe „wrc" auf Seite 154) oder über die Webschnittstelle gestartet werden.

Alle Aktionen werden unabhängig voneinander ausgeführt. Sie können eine oder mehrere Sitzungen derselben oder unterschiedlicher Aktionen gleichzeitig ausführen.

Beim Starten einer Aktion kann folgende Reaktionszeit festgelegt werden:

- Eine Sitzung wird ohne Benachrichtigung an den Benutzer des Zielrechners gestartet, wenn für die Reaktionszeit der Wert **0** festgelegt wurde.
- Wenn für die Reaktionszeit ein Wert **größer als 0** festgelegt wurde, wird auf dem Zielrechner ein Dialog angezeigt. Darin wird der Benutzer aufgefordert, die Sitzung zu akzeptieren. Wenn der Benutzer die Sitzung nicht innerhalb der Reaktionszeit akzeptiert, tritt, je nach den Einstellungen für die Zeitlimitüberschreitung, eine der folgenden beiden Situationen ein. Entweder wird die Sitzung gestartet, oder für den Administrator wird die Nachricht eingeblendet, dass das Zeitlimit für die Sitzung überschritten wurde.

  Wenn der Benutzer des Zielrechners die Sitzung ablehnt, wird auf dem Controller eine entsprechende Warnung angezeigt.

Die Reaktionszeit wird über die Standardrichtlinie festgelegt und kann von Ihnen geändert werden. Weitere Informationen finden Sie unter „Tivoli Remote Control-Richtlinienmethoden" auf Seite 74.

Über den Tivoli-Desktop starten

So starten Sie eine Aktion über den Tivoli-Desktop:

1. Doppelklicken Sie auf einen Richtlinienbereich.
2. Doppelklicken Sie auf das Remote Control-Tool.

Einer der beiden folgenden Dialoge wird angezeigt.

Dialog mit Zielmaschinenliste

Wenn der Dialog mit der Zielmaschinenliste angezeigt wird, können Sie eine Sitzung wie folgt starten:

1. Über die Schaltfläche **Einstellungen editieren** können Sie bei Bedarf die durch die Standardrichtlinie definierten Einstellungen ändern. Siehe „Sitzungseinstellungen anpassen" auf Seite 90.

   Sie können auch über die Schaltfläche **Zielmaschinenliste definieren** den Inhalt der Zielmaschinenliste ändern, falls diese Schaltfläche verfügbar ist. Siehe „Vorhandene Zielmaschinenliste über einen Dialog ändern" auf Seite 89.

2. Wählen Sie einen Zielrechner aus der Liste **Zielmaschinen** aus. Wenn hinter dem Zielmaschinennamen ein Pluszeichen (+) steht, bedeutet dies, dass es sich um einen Endpunkt handelt.
3. Wählen Sie eine Aktion aus der Liste **Aktionen** aus. Eine Beschreibung der verfügbaren Aktionen finden Sie in den Kapiteln 4 bis 7.
4. Klicken Sie auf die Schaltfläche **Ausführen**, um die Sitzung zu starten.

Sie können eine Sitzung auch starten, indem Sie eine Zielmaschine auswählen und anschließend auf eine Aktion doppelklicken oder indem Sie eine Aktion auswählen und anschließend auf eine Zielmaschine doppelklicken.

Dialog mit Richtlinienbereichs- und Zielmaschinenliste

Wenn der Dialog mit der Richtlinienbereichs- und Zielmaschinenliste angezeigt wird, können Sie den Inhalt der Zielmaschinenliste ändern, indem Sie einen Richtlinienbereich und eine Zielmaschinenart auswählen.

Führen Sie folgende Schritte aus, um eine Sitzung zu starten:

1. Über die Schaltfläche **Einstellungen editieren** können Sie bei Bedarf die durch die Standardrichtlinie definierten Einstellungen ändern. Siehe „Sitzungseinstellungen anpassen" auf Seite 90.
2. Wählen Sie im Listenfeld **Richtlinienbereichsmodus** die Richtlinienbereiche aus, die unter 'Richtlinienbereiche' angezeigt werden sollen.
3. Wählen Sie in der Liste **Richtlinienbereiche** den Richtlinienbereich aus, dessen Zielmaschinen unter 'Zielmaschinen' angezeigt werden sollen.
4. Wählen Sie einen Zielrechner aus der Liste **Zielmaschinen** aus.
5. Wählen Sie eine Aktion aus der Liste **Aktionen** aus. Eine Beschreibung der verfügbaren Aktionen finden Sie in den Kapiteln 4 bis 7.
6. Klicken Sie auf die Schaltfläche **Ausführen**, um die Sitzung zu starten.

Sie können eine Sitzung auch starten, indem Sie eine Zielmaschine auswählen und anschließend auf eine Aktion doppelklicken oder indem Sie eine Aktion auswählen und anschließend auf eine Zielmaschine doppelklicken. Informationen zur Konfiguration der Zielmaschinenliste in diesen Dialogen finden Sie unter „Zielmaschinenliste anpassen" auf Seite 87.

Über einen Web-Browser starten

So starten Sie eine Aktion über einen Web-Browser:

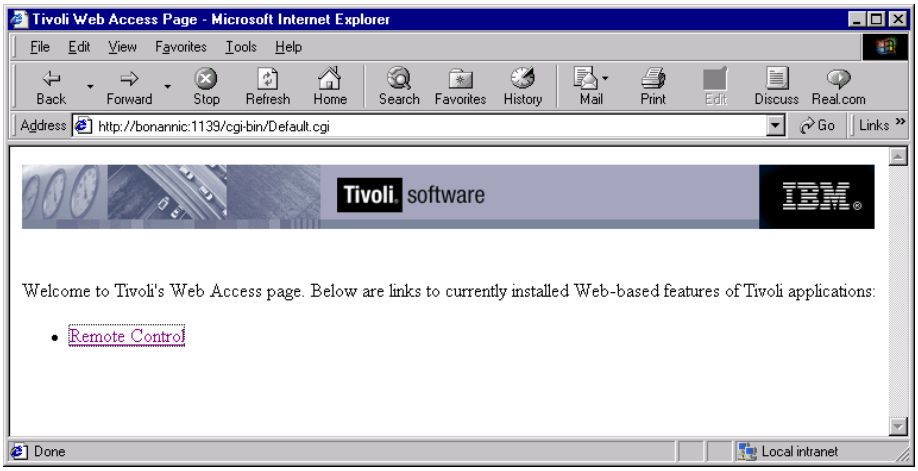
1. Öffnen Sie in einem Web-Browser folgende URL:

   ```
   http://TMR_Servername:TMR_Serverport
   ```

   TMR_Servername ist der Hostname des Tivoli-Servers, und TMR_Serverport ist die Nummer des Ports, an dem der Objektdispatcher empfangsbereit ist. Standardmäßig ist die Portnummer für den Objektdispatcherprozess 94. Beispiel für diese URL: http://alpha:94.

   Anmerkung: Der für `TMR_Serverport` angegebene Wert muss mit dem bei der Installation festgelegten Wert übereinstimmen. Weitere Informationen finden Sie im Handbuch *Tivoli Management Framework Planung und Installation*.

   Daraufhin wird eine Verbindung zum Tivoli-HTTP-Server hergestellt, der nur auf dem Tivoli-Server installiert ist. Die dynamisch generierte Standardseite 'default.cgi' wird angezeigt.


Tivoli Web Access Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Real.com
Address http://bonannic:1139/cgi-bin/Default.cgi
Go Links
Tivoli software
IBM
Welcome to Tivoli's Web Access page. Below are links to currently installed Web-based features of Tivoli applications:
Remote Control
Done
Local intranet

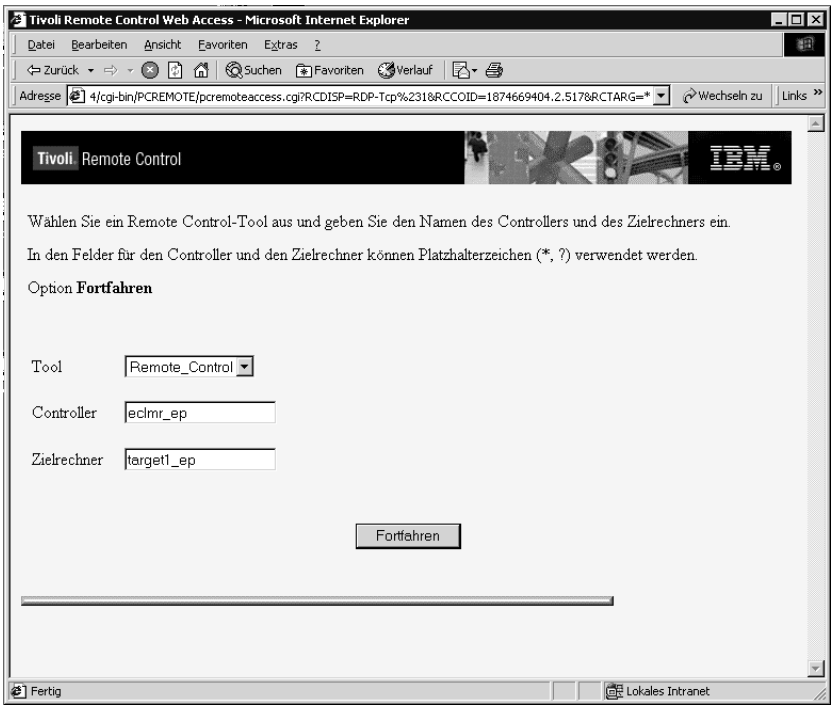
   Anmerkung: Unterstützt werden Internet Explorer 4 oder höher und Netscape 4.6 oder höher.

2. Klicken Sie auf den Link 'Remote Control'. Wenn Sie das erste Mal darauf klicken, wird im Web-Browser ein Fenster mit Textfeldern für den Benutzernamen und das Kennwort angezeigt. (Wenn der Link 'Remote Control' nicht angezeigt wird, wurde Remote Control nicht installiert.)

   Anmerkung: Wenn Sie die Tivoli Remote Control-Webschnittstelle zum zweiten Mal über Internet Explorer starten, werden Sie nicht aufgefordert, eine Benutzer-ID und ein Kennwort einzugeben, da Internet Explorer grundlegende HTTP-Authentifizierungszugriffstoken zwischenspeichert. Dies ist bei Netscape nicht der Fall. Deshalb sollte der Administrator Windows NT-, Windows XP- oder Windows 2000-Workstations, auf denen der Zugriff auf die Tivoli Remote Control-Webschnittstelle über Internet Explorer erfolgt, immer überwachen. Internet Explorer fordert nur beim Abmelden und Anmelden eine neue Authentifizierung an, nicht beim Schließen und erneuten Starten des Browsers.

3. Geben Sie die Benutzer-ID und das Kennwort eines Tivoli-Administrators ein, dessen Anmeldung auf dem TMR-Server (TMR = Tivoli Management Region) definiert ist, da der Tivoli-Webserver auf dem TMR-Server ausgeführt wird.

Wenn die Authentifizierung fehlschlägt, überprüfen Sie, ob Sie die in Kapitel 4, „Die Tivoli-Umgebung für die Verwendung der Tivoli Remote Control-Schnittstellen konfigurieren", auf Seite 65 beschriebenen Tasks ausgeführt haben. Folgende Seite wird angezeigt:



4. Wählen Sie das Tool aus und geben Sie den Namen des Controllers und des Zielrechners ein. Klicken Sie auf **Fortfahren**.

   Anmerkung: Wenn Sie sich nicht an den Namen des Controllers oder des Zielrechners erinnern, können Sie Platzhalterzeichen wie * und ? verwenden. Dabei gilt:

   ***** Steht für eine beliebige Zeichenfolge.

   ? Steht für ein beliebiges Zeichen.

Je nachdem, welche Werte Sie in die Felder für den Controller und den Zielrechner eingeben, wird eine der folgenden Seiten angezeigt:

Diese Seite wird angezeigt, wenn Sie die Namen für den Controller und den Zielrechner eingeben.

Diese Seite wird angezeigt, wenn Sie den Namen des Controllers eingeben und für die Bezeichnung des Zielrechners Platzhalterzeichen verwenden.

In diesem Fall müssen Sie noch einen Zielrechnernamen auswählen, da Sie im Textfeld **Zielrechner** auf der vorherigen Seite ein Platzhalterzeichen verwendet haben. Auf beiden Seiten werden die Standardwerte der restlichen Felder aus den Richtlinienmethoden des Richtlinienbereichs abgerufen, in dem sich das ausgewählte Tool befindet. Um die Standardwerte zu ändern, müssen die zugehörigen Richtlinienmethoden editiert werden.

5. Klicken Sie auf eine der Schaltflächen, um die gewünschte Tivoli Remote Control-Aktion zu starten.

Unter Windows 2000, Windows NT, Windows XP und Windows 98 Second Edition können Sie die Tivoli Remote Control-Webschnittstelle starten, indem Sie Folgendes ausführen:

```
<lcf>\PCREMOTE\<i>\CTL\TRCWTS.EXE
```

Dabei gilt:

<lcf>	ist das Installationsverzeichnis des Tivoli-Managementagenten.
<i>	kann einen der folgenden Werte annehmen: • 'w32-ix86' für Windows NT, Windows 2000 und Windows XP • 'win95' für Windows 98 Second Edition

Im Textfeld für den Controller wird automatisch der Name des Endpunkts angezeigt, auf dem TRCWTS.EXE ausgeführt wurde.

Über eine Terminal Server-Umgebung starten

Sie können eine Tivoli Remote Control-Aktion auch von einem Controller aus starten, der ein Terminal Client ist. Führen Sie dazu bei aktiver Windows Terminal Server-Sitzung die Datei TRCWTS.EXE in folgendem Verzeichnis aus:

```
<lcf>\PCREMOTE\w32-ix86\CTL
```

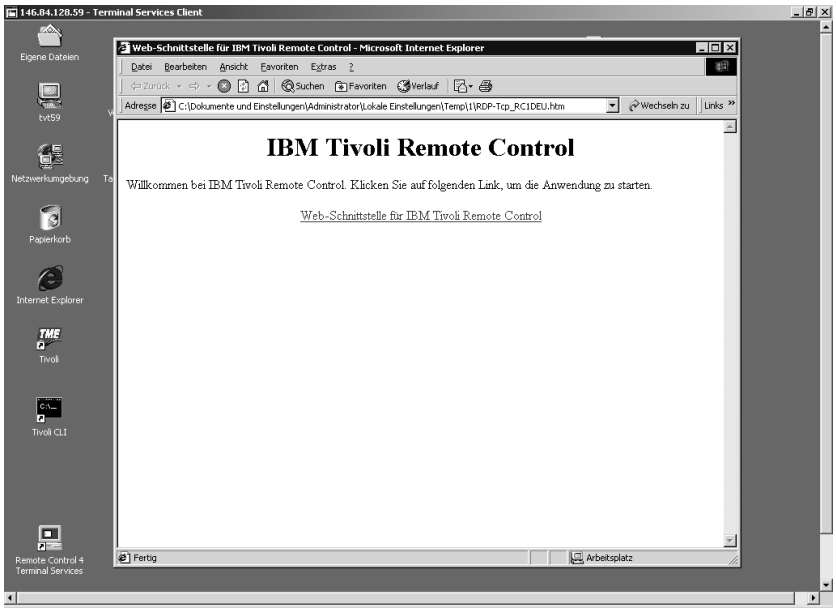
Dabei gilt:

<lcf>	ist das Installationsverzeichnis des Tivoli-Managementagenten.
w32-ix86	gilt nur, wenn Windows Terminal Server unterstützt wird.

Eine Sitzung über einen Terminal Server starten

Anmerkung: Stellen Sie sicher, dass TRCWTS.EXE vom Verzeichnis <lcf>\PCREMOTE\<w32-ix86>\CTL aus ausgeführt wird, und verschieben Sie dieses Programm nicht in ein anderes Verzeichnis.

Im standardmäßigen Web-Browser wird die Standardseite für Remote Control Windows Terminal Server (WTS) geöffnet.



Führen Sie in der Windows Terminal Server-Konsole folgende Schritte aus, um die Webschnittstellenseite anzupassen:

1. Erstellen Sie für die Datei TRCWTS.EXE einen Direktaufruf auf dem Desktop.
2. Öffnen Sie die Eigenschaften des Direktaufrufs für TRCWTS.
3. Im Feld **Zielrechner**, in dem TRCWTS.EXE aufgeführt ist, können Sie mit der in „Tivoli Remote Control-Webseite anpassen" auf Seite 91 beschriebenen Syntax weitere Parameter angeben.

Die Datei TRCWTS.EXE kann auch über die Befehlszeile ausgeführt werden.

Zum Starten der Dateiübertragung und des Chats von einem Windows Terminal Services Client aus muss der derzeit angemeldete Benutzer Schreib- und Lesezugriff für das Installationsverzeichnis des Produkts haben. Wenn der Benutzer nicht über diese Zugriffsberechtigungen verfügt, werden Aktionen, bei denen Dateien erstellt oder geändert werden (z. B. Protokolldateien für Chat und Dateiübertragung, Tracedateien usw.), nicht ausgeführt und können zu einem Abbruch der Sitzung führen.

Über die Befehlszeile starten

Die Befehlszeilenschnittstelle (CLI) wird normalerweise von anderen Anwendungen zum Ausführen von Tivoli Remote Control-Aktionen verwendet. Sie können auch selbst CLI-Befehle eingeben. Weitere Informationen zum Befehl und zur Syntax, die zum Starten einer Sitzung verwendet werden, finden Sie unter „wrc" auf Seite 154.

Tivoli Remote Control-Gateway starten

Das Remote Control-Gateway ist ein Hintergrundprozess, der auf dem verwalteten Knoten ausgeführt wird, auf dem der Remote Control-Server installiert wurde und die Richtlinienmethode 'rc_def_gw' konfiguriert wurde. Er wird gestartet, sobald eine Tivoli Remote Control-Sitzung beginnt, die dieses Gateway benötigt.

Tivoli Remote Control-Proxy starten

Führen Sie folgende Schritte aus, um den Remote Control-Proxy zu starten:

Auf Windows-Systemen:

1. Öffnen Sie in der Systemsteuerung 'Dienste'.
2. Wählen Sie aus der Liste der Dienste den Remote Control-Proxy aus.
3. Wählen Sie aus dem Kontextmenü **Starten** aus.

Auf UNIX-Systemen:

Geben Sie im Installationsverzeichnis des Remote Control-Proxys folgenden Befehl ein:

```
./rcproxy
```

Anmerkung: Der Tivoli Remote Control-Proxyprozess wird auf Unix-Plattformen im Vordergrund gestartet.

Weitere Informationen zu den Befehlen, die Sie zur Verwaltung des Remote Control-Proxys ausführen können, finden Sie unter „rcproxy" auf Seite 150.

Remote Control-Gateway und Remote Control-Proxy starten

Kapitel 9. Aktionen 'Remote Control' und 'Neustart' verwenden

In diesem Kapitel wird die Verwendung der Aktion 'Remote Control' (Fernsteuerungsaktion) zum Überwachen oder Steuern eines Zielrechners beschrieben. Außerdem wird erläutert, wie Sie einen Zielrechner mit Hilfe der Aktion 'Neustart' neu starten können.

Die Remote Control-Sitzung ist von anderen Aktionen in Tivoli Remote Control unabhängig und kann gleichzeitig mit Dateiübertragungs- und Chat-Sitzungen ausgeführt werden.

Sie können auch mehrere Remote Control-Sitzungen gleichzeitig ausführen.

Aktion 'Remote Control' verwenden

Mit Hilfe der Aktion 'Remote Control' können Sie die Bildschirmanzeige einer oder mehrerer Zielrechner gleichzeitig anzeigen. Jeder Zielrechner wird in einem eigenen Fenster angezeigt. In der Titelleiste des Fensters wird der Name des aktuellen Zielrechners angezeigt.

Remote Control-Sitzungen starten und beenden

Wählen Sie zum Starten einer Remote Control-Sitzung die Remote Control-Aktion wie unter „Eine Tivoli Remote Control-Aktion starten" auf Seite 93 beschrieben aus.

Beim Start der Sitzung ist der Status entsprechend der Einstellung für den Anfangsstatus entweder **Aktivieren** oder **Überwachen**. Siehe „Sitzungseinstellungen anpassen" auf Seite 90. Die Status werden unter „Sitzungsstatus ändern" auf Seite 102 näher erläutert.

Der Sitzungsstatus, der Tastaturmodus und der Verschlüsselungsmodus werden je nach Betriebssystem des Controllers entweder in der Statusleiste oder in der Titelleiste angezeigt.

Wählen Sie im Menü 'Datei' die Option **Beenden** aus, um eine Remote Control-Sitzung zu schließen.

Das Fenster 'Remote Control'

Während einer Remote Control-Sitzung wird das Fenster 'Remote Control' auf dem Controller angezeigt.

Es enthält folgende Menüs:

Datei Enthält Optionen zum Speichern des Zielrechnerbildschirms als Bitmap, zum Ausdrucken des Fensterinhalts auf dem Standarddrucker, zum Anzeigen einer Druckvoranzeige eines Dokuments (unter OS/2 nicht möglich) und zum Verlassen des Fensters, um zu den Zielmaschinenlisten zurückzukehren.

Tastenkombinationen
Enthält Optionen zum Umschalten in andere Tastaturmodi und zum Senden von Tastenkombinationen an den Zielrechner. Weitere Informationen finden Sie unter „In andere Tastaturmodi umschalten" auf Seite 104 und „Systemtastenkombinationen senden" auf Seite 104.

Status Enthält Optionen zum Umschalten in die Status 'Aktivieren', 'Überwachen' und 'Suspendieren'. Weitere Informationen finden Sie unter „Status vom Controller aus ändern".

Anzeigen Enthält Optionen zum Ein- oder Ausblenden der Funktionsleiste und Statusleiste. Dieses Menü ist unter OS/2 nicht verfügbar.

Hilfe Enthält Informationen zu Tivoli Remote Control.

Sitzungsstatus ändern

Der Sitzungsstatus kann entweder vom Administrator oder vom Zielrechnerbenutzer geändert werden.

Status vom Controller aus ändern

Wählen Sie zum Ändern des Sitzungsstatus die gewünschte Option im Menü **Status** aus.

Aktivieren Übernimmt die Steuerung von Tastatur und Maus des Zielrechners. Der Zielrechnerbenutzer kann die Maus und die Tastatur erst wieder bedienen, wenn er die Tastenkombination <Alt><T> drückt (sofern er dazu berechtigt ist). In diesem Fall bleibt die Steuerung durch den Controller so lange gesperrt, bis der Zielrechnerbenutzer einen neuen Status auswählt. Wenn für die Sitzung ein Inaktivitätszeitlimit festgelegt wurde, muss die Maus bewegt oder die Tastatur verwendet werden, damit die Sitzung nicht beendet wird.

Überwachen Zeigt auf dem Controller den Bildschirminhalt des Zielrechners an. Der Controllerbenutzer kann jedoch über die Tastatur oder Maus keine Eingaben an dem Zielrechner vornehmen.

Suspendieren
Inaktiviert die Sitzung. Die Verbindung zum Zielrechner bleibt dabei zwar bestehen, doch der Controllerbenutzer kann weder den Zielrechner steuern noch die aktualisierte Bildschirmanzeige sehen. Er kann zum Status 'Aktivieren' oder 'Überwachen' zurückkehren, ohne die Sitzung erneut zu starten.

Beenden Beendet die Sitzung und die Verbindung zum Controller.

Der Status **Aktivieren** ist in folgenden Fällen nicht verfügbar:

- Sie als Controllerbenutzer verfügen auf dem Zielrechner nur über die Berechtigungsklasse **remote_monitor**. Siehe „Schritt 3: Tivoli Remote Control-Berechtigungsklassen zuordnen" auf Seite 69.
- Mit der Richtlinienmethode **rc_def_rcmode** wird nur der Überwachungsmodus angegeben. Siehe Seite 83.

Status vom Zielrechner aus ändern

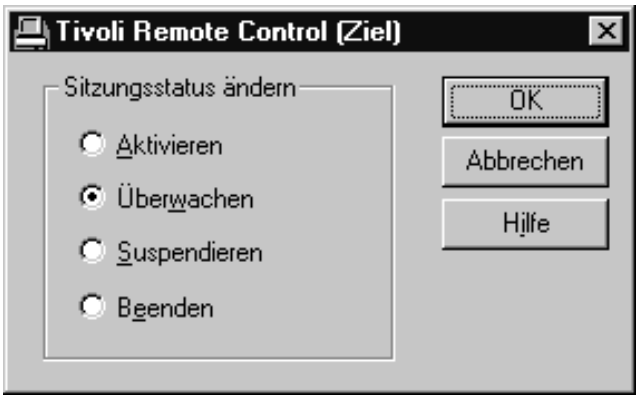
Während einer Sitzung kann, abhängig vom Sitzungsstatus, eines der folgenden Symbole auf dem Zielrechner angezeigt werden. Der Standardwert wird durch die Richtlinienmethode **rc_def_alt_t** festgelegt (siehe Seite 75).

- In der Taskleiste eines Windows-Zielrechners:

- Auf dem Desktop eines OS/2-Zielrechners (falls aktiviert):

Folgender Dialog wird angezeigt, wenn der Zielrechnerbenutzer die Tastenkombination <Alt><T> drückt sowie in folgenden Fällen:

- Unter Windows klickt der Zielrechnerbenutzer auf das Symbol ALT+T.
- Unter OS/2 doppelklickt der Zielrechnerbenutzer auf das Symbol ALT+T.



Anschließend kann der Zielrechnerbenutzer den Sitzungsstatus ändern. Erläuterungen zu den verschiedenen Status finden Sie unter „Status vom Controller aus ändern" auf Seite 102.

In andere Tastaturmodi umschalten

Das Umschalten in andere Tastaturmodi ist nur im aktiven Status möglich. Folgendes gilt im aktiven Status:

- Im Tastaturmodus **FERNE TASTENKOMBINATIONEN** wird die Tastatureingabe an den Zielrechner gesendet.
- Im Tastaturmodus **LOKALE TASTENKOMBINATIONEN** wirkt sich die Tastatureingabe nur lokal aus.

Zum Umschalten in andere Tastaturmodi können Sie eine der folgenden Aktionen ausführen:

- Drücken Sie die Tastenkombination <Alt><T>.
- Wählen Sie im Menü **Tastenkombinationen** die Option **Modus umschalten auf fern** bzw. **Modus umschalten auf lokal** aus.

Systemtastenkombinationen senden

Einige Tastenkombinationen können nicht über die Tastatur an den Zielrechner gesendet werden, da sie vom lokalen Betriebssystem verarbeitet werden. Diese Tastenkombinationen können Sie jedoch senden, indem Sie im Menü **Tastenkombinationen** die Option 'Systemtastenkombinationen senden' auswählen. Anschließend können Sie die gewünschte Option auswählen oder auf das entsprechende Symbol klicken.

Die Auswirkung einer Tastenkombination richtet sich nach dem Betriebssystem des Zielrechners. Die folgenden Beispiele für Tastenkombinationen gelten für Windows-Plattformen.

Alt+Esc	Wechselt auf dem Zielrechner in das nächste Fenster.
Alt+Tab	Wechselt auf dem Zielrechner in das vorherige Fenster.
Strg+Esc	Zeigt auf dem Zielrechner den Dialog 'Taskliste' an.

In andere Tastaturmodi umschalten und Systemtastenkombinationen senden

Anmerkung: Die unter Windows verfügbare Funktion der Schaltfläche**Start** zum Anzeigen der Taskleiste kann nicht an den Zielrechner gesendet werden. Verwenden Sie stattdessen die Tastenkombination **Strg+Esc**.

Strg+Umschalt+Esc Aktiviert den Task-Manager (nur auf Zielrechnern mit Windows NT 4.0, Windows 2000 oder Windows XP).

Strg+Alt+Entf Zeigt auf Windows NT-, Windows 2000- und Windows XP-Zielrechnern den Dialog 'Sicherheit' und auf Windows 98 Second Edition-Zielrechnern den Dialog 'Anwendung schließen' an. Diese Option ist auf OS/2-Zielrechnern nicht verfügbar.

Anmerkung: Wenn die Sitzung nicht ordnungsgemäß beendet wird, während Sie von einem Controller aus bei einem Windows NT-, Windows 2000- oder Windows XP-Zielrechner angemeldet sind, werden Sie automatisch abgemeldet. Ein angemeldeter Zielrechnerbenutzer wird bei einem nicht ordnungsgemäßen Beenden der Sitzung jedoch nicht automatisch abgemeldet.

IME-Sprungtaste Aktiviert bzw. inaktiviert auf DBCS-Zielrechnern den IME (Input Method Editor, in asiatischen Ländern verwendetes Zeichendarstellungssystem). Diese Option ist bei SBCS-Zielrechnern (SBCS = Zeichendarstellungssystem für westliche Sprachen) inaktiviert.

Einschränkungen bei der Tastatureingabe auf einem OS/2-Gateway

Wenn ein Controller oder ein Zielrechner auf einem Endpunkt installiert ist, der gleichzeitig auch als OS/2-Gateway dient, kann es zu Problemen bei der Tastatureingabe kommen. Legen Sie in diesem Fall das folgende Feld in der Datei 'config.sys' wie angegeben fest:

```
TRUSTEDPATH=NO
```

Beachten Sie jedoch, dass dadurch ein Neustart erforderlich ist und die Anmeldung am Tivoli-Gateway inaktiviert wird.

Verschiedene Tastaturen verwenden

Tivoli Remote Control unterstützt die Tastenkonvertierung zwischen einem Controller und einem Zielrechner mit unterschiedlichen Tastaturen, d. h. wenn Sie eine Taste auf der Tastatur des Controllers drücken, wird das zugeordnete Zeichen auf dem Zielrechnerbildschirm angezeigt. Für die Tastenkonvertierung bestehen folgende Einschränkungen:

- Damit die Taste einer Controllertastatur konvertiert werden kann, muss das zugeordnete Zeichen auf der Zielrechnertastatur vorhanden sein.

Verschiedene Tastaturen verwenden

- Einige Tastenkombinationen auf der Controllertastatur werden auf dem Zielrechnerbildschirm in andere Zeichen konvertiert. Was passiert beispielsweise, wenn Sie auf einer französischen Tastatur ein Akzentzeichen gefolgt von einem Vokal eingeben? Als Ergebnis werden auf dem Controllerbildschirm ein einziges Zeichen (der akzentuierte Vokal), auf dem Zielrechnerbildschirm jedoch zwei Zeichen (das Akzentzeichen und der Vokal) angezeigt.

In der folgenden Tabelle sind die Tastaturarten aufgeführt, für die Tivoli Remote Control die Tastenkonvertierung unterstützt. Die in einer Zeile aufgeführten Tastaturbezeichnungen stehen immer für dieselbe Tastaturart. Die hier aufgeführten Tastaturbezeichnungen entsprechen den Bezeichnungen in den jeweiligen Betriebssystemen für diese Tastaturart.

Windows NT **Windows 2000** **Windows XP**	**Windows 98 Second Edition**	**OS/2**
Belgisches Französisch	Belgisch	Belgisch
Brasilianisch (ABNT)	Portugiesisch (Brasilien) (ABNT2)	Brasilianisch (275)
Chinesisch (Vereinfacht)	Chinesisch (Vereinfacht)	Chinesisch (Vereinfacht)
Chinesisch (Traditionell)	Chinesisch (Traditionell)	Chinesisch (Traditionell)
Französisch	Französisch	Französisch
Deutsch	Deutsch	Deutsch
Italienisch	Italienisch	Italienisch
Japanisch (5576-002) (5576-003) (5576-A01) (5576-B01) (5576-B05) (5576-C01)	Japanisch (5576-002) (5576-003) (5576-A01) (5576-B01) (5576-B05) (5576-C01)	Japanisch (5576-002) (5576-003) (5576-A01) (5576-B01) (5576-B05) (5576-C01)
Koreanisch	Koreanisch	Koreanisch
US	US	USA
US-Dvorak	US-Dvorak	
US-International	US-International	

Tastaturen synchronisieren

Während einer aktiven Remote Control-Sitzung wird der Status der Sperrtasten (wie <Num>, <Rollen> und <Feststelltaste>) der Zielrechnertastatur mit dem Status der entsprechenden Tasten auf der Controllertastatur synchronisiert.

Der Status der Sperrtasten auf der Zielrechnertastatur wird in folgenden Fällen auf seinen ursprünglichen Wert zurückgesetzt:

- Die Remote Control-Sitzung wird beendet.
- Der Sitzungsstatus ändert sich von 'Aktivieren' zu 'Überwachen'.

Aktion 'Neustart' verwenden

Wählen Sie zum erneuten Starten eines Zielrechners von einem Controller aus die Aktion 'Neustart' wie unter „Eine Tivoli Remote Control-Aktion starten" auf Seite 93 beschrieben aus.

Bei einem Zielrechner mit mehreren Neustartmöglichkeiten findet der Neustart unter dem standardmäßigen Betriebssystem statt.

Kapitel 10. Aktion 'Chat' verwenden

In diesem Kapitel wird die Verwendung der Aktion 'Chat' zum Austauschen von Nachrichten mit dem Zielrechnerbenutzer beschrieben.

Die Chat-Sitzung ist von anderen Aktionen in Tivoli Remote Control unabhängig und kann gleichzeitig mit Remote Control- und Dateiübertragungssitzungen ausgeführt werden. Sie kann nicht über Firewalls hinweg über die Remote Control-Proxys ausgeführt werden.

Stellen Sie vor der Ausführung einer Chat-Sitzung sicher, dass auf Ihrer Workstation mindestens 256 Farben angezeigt werden.

Chat-Sitzungen starten und beenden

Wählen Sie zum Starten einer Chat-Sitzung die Aktion 'Chat' wie unter „Eine Tivoli Remote Control-Aktion starten" auf Seite 93 beschrieben aus. Sie können eine oder mehrere Chat-Sitzungen gleichzeitig ausführen.

Bei Sitzungsbeginn wird das Fenster 'Chat' sowohl auf dem Controller als auch auf dem Zielrechner angezeigt. Siehe „Das Fenster 'Chat'".

Die Chat-Sitzung kann vom Administrator oder vom Zielrechnerbenutzer geschlossen werden.

Wenn Sie eine Sitzung schließen möchten, klicken Sie entweder auf das Symbol für 'Beenden' oder wählen Sie im Menü 'Aktionen' die Option 'Beenden' aus. Das Fenster 'Chat' wird sowohl auf dem Controller als auch auf dem Zielrechner geschlossen.

Das Fenster 'Chat'

Während einer Chat-Sitzung wird das Fenster 'Chat' sowohl auf dem Controller als auch auf dem Zielrechner angezeigt. Auf dem Zielrechner wird in der Titelleiste der Name des Controllers angezeigt. Auf dem Controller wird der Name des Zielrechners angezeigt.

Chat-Sitzungen ausführen

Das Fenster 'Chat' enthält als Hauptbestandteile den Sendebereich und den Protokollbereich. Sie können die horizontale Trennlinie zwischen Protokoll- und Sendebereich durch Anklicken und Ziehen nach oben und unten verschieben.

Im Sendebereich wird der Text angezeigt, den Sie senden möchten. Im Protokollbereich werden alle Nachrichten der aktuellen Unterhaltung in chronologischer Reihenfolge angezeigt.

In der folgenden Tabelle werden die Menüs und Symbole des Fensters erläutert.

Symbol	Menüoption	Funktion
	Aktionen → Suspendieren	Inaktiviert die Chat-Sitzung auf Controller und Zielrechner.
	Aktionen → Aktivieren	Aktiviert die Chat-Sitzung auf Controller und Zielrechner.
	Aktionen → Beenden	Beendet die Chat-Sitzung.
	Aktionen → Protokollieren	Aktiviert die Protokollierung der Chat-Nachrichten.
	Aktionen → Nicht protokollieren	Inaktiviert die Protokollierung der Chat-Nachrichten.
	Editieren → Senden	Sendet den im Sendebereich eingegebenen Text an den Zielrechner.
	Editieren → Inhalt löschen	Löscht den im Sendebereich eingegebenen Text.
	Hilfe → Hilfethemen	Zeigt die Onlinehilfe an.

Nachrichten austauschen

So senden Sie eine Nachricht vom Controller oder vom Zielrechner aus:

1. Geben Sie im Sendebereich den Text ein. Sie können Text in gewohnter Weise kopieren und einfügen und die Tasten <Rückschritt>, <Entf> und <Tabulator> zum Editieren verwenden. Mit der Tastenkombination <Strg><Umschalt><Entf> können Sie Text löschen.
2. Drücken Sie entweder die <Eingabetaste>, oder klicken Sie auf das Symbol für 'Senden', oder wählen Sie im Menü 'Editieren' die Option 'Senden' aus.

Daraufhin wird die Nachricht sowohl im Protokollbereich des Senders als auch des Empfängers angezeigt.

Der Empfänger kann nun seinerseits im Sendebereich eine Antwort schreiben und diese senden. Obwohl der Protokollbereich schreibgeschützt ist, können Sie dort Textstellen in gewohnter Weise kopieren.

Nachfolgende Nachrichten werden hinter den bereits vorhandenen Nachrichten im Protokollbereich angefügt.

Wenn die Protokollfunktion aktiviert wurde, werden die Einzelheiten des Dialogs in der Chat-Protokolldatei festgehalten. Siehe „Chat-Dialoge protokollieren" auf Seite 110 weiter unten.

Chat-Sitzungen suspendieren und erneut aktivieren

Wenn Sie eine Chat-Sitzung suspendieren, d. h. inaktivieren möchten, klicken Sie entweder auf das Symbol für 'Suspendieren', oder wählen Sie im Menü 'Aktionen' die Option 'Suspendieren' aus. Daraufhin wird der Sendebereich sowohl auf dem Controller als auch auf dem Zielrechner inaktiviert.

Wenn Sie den Sendebereich erneut aktivieren möchten, klicken Sie entweder auf das Symbol für 'Aktivieren' oder wählen Sie im Menü 'Aktionen' die Option 'Aktivieren' aus. Wenn Sie das Chat-Fenster auf Symbolgröße verkleinern oder in den Hintergrund stellen, ist der Sendebereich ebenfalls inaktiviert. Wenn Sie eine Nachricht empfangen, während das Chat-Fenster auf Symbolgröße verkleinert ist, werden Sie durch eine Systemnachricht darüber informiert.

Anmerkung: Wenn auf Ihrer lokalen Workstation folgende Fälle auftreten, wechselt die ferne Workstation, mit der Sie sich in einer Chat-Sitzung befinden, in den Status **Suspendieren**.

- Das Chat-Fenster befindet sich im Hintergrund.
- Das Chat-Fenster ist minimiert.
- Der Bildschirmschoner wurde gestartet.

Chat-Dialoge protokollieren

Wenn Sie den Chat-Dialog protokollieren lassen möchten, klicken Sie entweder auf das Symbol für 'Protokollieren', oder wählen Sie im Menü 'Aktionen' die Option 'Protokollieren' aus (**Aktionen -> Protokollieren**).

Wenn Sie die Protokollierung aktivieren, wird ein Dialog angezeigt, in dem Sie die Position der neuen Protokolldatei RC_CHAT.LOG auswählen können. Die Standardposition ist das Installationsverzeichnis von Tivoli Remote Control.

Chat-Ereignisse protokollieren

Während einer Chat-Sitzung können Sie informative Ereignisse und Fehler protokollieren. Die Protokollierung der Chat-Ereignisse wird automatisch aktiviert. Sie können die Protokollstufe der aktuellen Sitzung zur Laufzeit anpassen, indem Sie im F2 drücken. Daraufhin wird folgendes Dialogfeld angezeigt:

Sie können eine der folgenden Protokollstufen auswählen:
- Aus
- Fehler
- Warnung
- Informationen

Die Chat-Ereignisse werden in den folgenden Dateien protokolliert:
- *<lcf>*\PCREMOTE*<i>*\CTL\Logs\RCCTL_CH*JJJJMMTT@hhmmss*.log auf dem Controller.

  Dabei gilt:

<lcf>	ist das Installationsverzeichnis des Tivoli-Managementagenten.
<i>	kann einen der folgenden Werte annehmen: – 'w32-ix86' für Windows NT, Windows 2000 und Windows XP – 'win95' für Windows 98 Second Edition – 'os2-ix86' für OS/2
JJJJMMTT	steht für das Jahr (4 Ziffern), den Monat (2 Ziffern) und den Tag (2 Ziffern). Beispiel: 20021105.
hhmmss	steht für die Stunden (2 Ziffern), Minuten (2 Ziffern) und Sekunden (2 Ziffern). Beispiel: 153350.

- *<lcf>*\PCREMOTE*<i>*\TGT\Logs\RCTGT_CH*JJJJMMTT@hhmmss*.log auf dem Zielrechner.

Weitere Informationen finden Sie unter „Chat-Ereignisse auf dem Controller und auf dem Zielrechner protokollieren" auf Seite 119.

Chat bei Remote Control-Sitzungen verwenden

Wenn Sie eine Chat-Sitzung starten, während sich eine Remote Control-Sitzung im aktiven Status befindet, wird die Remote Control-Sitzung automatisch suspendiert. Der Zielrechnerbenutzer kann die Tastatur und die Maus dann zur Bedienung der Chat-Sitzung verwenden.

In folgenden Fällen wird die Remote Control-Sitzung erneut aktiviert:

- Die Chat-Sitzung wird geschlossen oder suspendiert.
- Der Zielrechnerbenutzer wählt eine andere Anwendung aus.

Wenn Sie eine Chat-Sitzung starten, während sich eine Remote Control-Sitzung im Überwachungsstatus befindet, werden beide Sitzungen normal ausgeführt.

Chat-Sitzungen ausführen

Kapitel 11. Aktion 'Dateiübertragung' verwenden

In diesem Kapitel wird die Verwendung der Dateiübertragungsaktion zum Übertragen von Dateien oder Verzeichnissen zwischen Controller und Zielrechner beschrieben.

Die Dateiübertragungssitzung ist von anderen Aktionen in Tivoli Remote Control unabhängig und kann gleichzeitig mit Remote Control- und Chat-Sitzungen ausgeführt werden.

Stellen Sie vor der Ausführung einer Dateiübertragungssitzung sicher, dass auf Ihrer Workstation mindestens 256 Farben angezeigt werden.

Anmerkung: Die Dateiübertragungsaktion kann auf OS/2-Plattformen mit aktivierter Verschlüsselung nur auf einer HPFS-Partition ausgeführt werden.

Dateiübertragungssitzungen starten und beenden

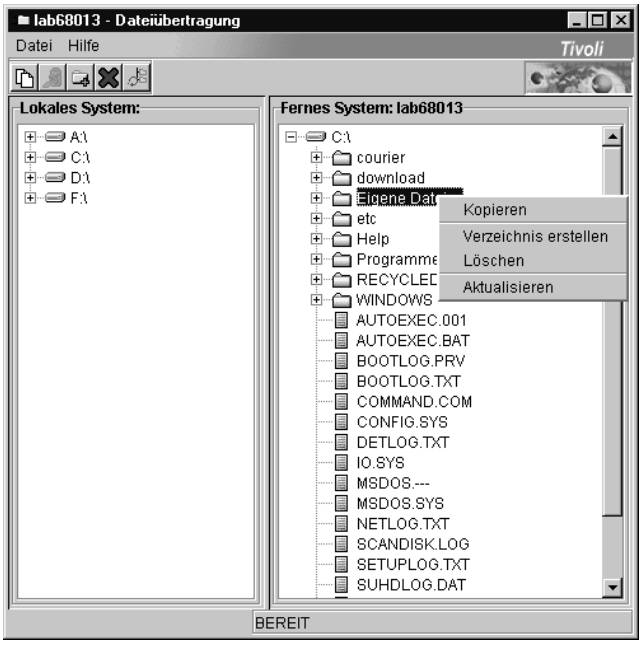
Wählen Sie zum Starten einer Dateiübertragungssitzung die Aktion 'Dateiübertragung' wie unter „Eine Tivoli Remote Control-Aktion starten" auf Seite 93 beschrieben aus. Sie können mehrere Dateiübertragungssitzungen gleichzeitig ausführen.

Bei Sitzungsbeginn wird das Fenster 'Dateiübertragung' auf dem Controller angezeigt. Siehe „Das Fenster 'Dateiübertragung'" auf Seite 114.

Wenn Sie eine Dateiübertragungssitzung schließen möchten, wählen Sie im Menü 'Datei' die Option 'Beenden' aus.

Das Fenster 'Dateiübertragung'

Während einer Dateiübertragungssitzung wird das Fenster 'Dateiübertragung' auf dem Controller angezeigt. In der Titelleiste wird der Name des Zielrechners eingeblendet.



Das Fenster 'Dateiübertragung' enthält als Hauptbestandteile den lokalen Systembereich und den fernen Systembereich. Sie können die vertikale Trennlinie zwischen Indexstruktur und Berichtsanzeige durch Anklicken und Ziehen nach rechts und links verschieben.

Im **lokalen Systembereich** wird das Dateisystem des Controllers angezeigt. Im **fernen Systembereich** wird das Dateisystem des Zielrechners angezeigt.

Um ein Verzeichnis zu erweitern bzw. zu komprimieren, doppelklicken Sie in gewohnter Weise darauf.

In der folgenden Tabelle werden die Menüs und Symbole des Fensters erläutert. Viele dieser Optionen sind ebenfalls über ein Kontextmenü verfügbar, das angezeigt wird, wenn Sie mit der rechten Maustaste auf den Fensterbereich klicken.

Symbol	Menüoption	Funktion
	Datei → Kopieren	Legt die Quelldateien oder -verzeichnisse für den Kopiervorgang fest.
	Datei → Einfügen	Legt das Zielverzeichnis fest und startet den Kopiervorgang. Die Auswahl eines Zielverzeichnisses ist erst möglich, wenn eine Quelle ausgewählt wurde.
	Datei → Verzeichnis erstellen	Erstellt im ausgewählten Verzeichnis ein neues Unterverzeichnis.
	Datei → Löschen	Löscht die ausgewählten Dateien oder Verzeichnisse.

Symbol	Menüoption	Funktion
	Datei → Aktualisieren	Aktualisiert die Anzeige des ausgewählten Verzeichnisses.
	Hilfe → Hilfethemen	Zeigt die Onlinehilfe an.

Dateien kopieren

Die Dateiübertragungsaktion ermöglicht das Kopieren und Einfügen ausgewählter Verzeichnisse oder Dateien zwischen zwei Maschinen, auf denen gleichzeitig eine Dateiübertragungssitzung ausgeführt wird.

Folgen Sie einer der folgenden Vorgehensweisen, um eine Verzeichnisstruktur oder Datei zu kopieren. In beiden Fällen können Sie eine Datei oder ein Verzeichnis auswählen, indem Sie auf das jeweilige Symbol klicken. Sie können in gewohnter Weise auch mehrere Elemente auswählen, indem Sie beim Klicken die <Umschalttaste> bzw. die <Strg-Taste> gedrückt halten.

So übertragen Sie Dateien oder Verzeichnisse mit Ziehen und Ablegen:

1. Wählen Sie die Dateien oder die Verzeichnisstruktur als Quelle aus, und ziehen und übergeben Sie diese in der neuen Position.

So übertragen Sie Dateien oder Verzeichnisse über Menüoptionen:

1. Wählen Sie die Dateien oder die Verzeichnisstruktur mit Hilfe der Option 'Kopieren' im Menü 'Datei' als Quelle aus.
2. Wählen Sie die Zielposition mit Hilfe der Option 'Einfügen' im Menü 'Datei' aus. Die Dateiübertragung wird gestartet, wenn Sie auf die Einfügefunktion klicken.

Verzeichnisse erstellen

So erstellen Sie ein neues Verzeichnis:

1. Wählen Sie das übergeordnete Verzeichnis für das neue Verzeichnis aus.
2. Klicken Sie entweder auf das Symbol für 'Verzeichnis erstellen', oder wählen Sie die gleichnamige Menüoption aus. Daraufhin wird der Dialog 'Verzeichnis erstellen' angezeigt.
3. Geben Sie den Namen des neuen Verzeichnisses ein, und klicken Sie auf 'OK'.

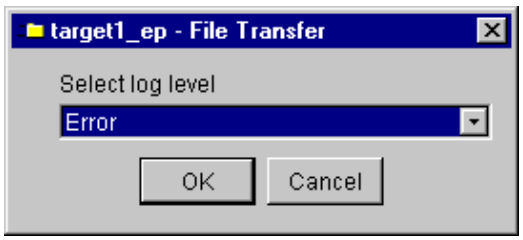
Verzeichnisse und Dateien löschen

So löschen Sie eine Datei oder ein Verzeichnis:

1. Wählen Sie die Datei oder das Verzeichnis aus. Sie können in gewohnter Weise auch mehrere Elemente auswählen, indem Sie beim Klicken die <Umschalttaste> bzw. die <Strg-Taste> gedrückt halten.
2. Klicken Sie entweder auf das Symbol für 'Löschen', oder wählen Sie die gleichnamige Menüoption oder Kontextmenüoption aus, oder drücken Sie die Taste 'Entf'.
3. Klicken Sie auf 'Ja'.

Dateiübertragungsereignisse protokollieren

Während einer Dateiübertragungssitzung können Sie informative Ereignisse und Fehler protokollieren. Die Protokollierung der Dateiübertragungsereignisse wird automatisch aktiviert. Sie können auf dem Controller die Protokollstufe der aktuellen Sitzung zur Laufzeit anpassen, indem Sie F2 drücken. Daraufhin wird folgendes Dialogfeld angezeigt:



Sie können eine der folgenden Protokollstufen auswählen:
- Aus
- Fehler
- Warnung
- Informationen

Die Dateiübertragungsereignisse werden in den folgenden Dateien protokolliert:
- *<lcf>*\PCREMOTE*<i>*\CTL\Logs\RCCTL_FT*JJJJMMTT@hhmmss*.log auf dem Controller.

  Dabei gilt:

<lcf>	ist das Installationsverzeichnis des Tivoli-Managementagenten.
<i>	kann einen der folgenden Werte annehmen: – 'w32-ix86' für Windows NT, Windows 2000 und Windows XP – 'win95' für Windows 98 Second Edition – 'os2-ix86' für OS/2
JJJJMMTT	steht für das Jahr (4 Ziffern), den Monat (2 Ziffern) und den Tag (2 Ziffern). Beispiel: 20021105.
hhmmss	steht für die Stunden (2 Ziffern), Minuten (2 Ziffern) und Sekunden (2 Ziffern). Beispiel: 153350.

- *<lcf>*\PCREMOTE*<i>*\TGT\Logs\RCTGT_FT.log auf dem Zielrechner.

Weitere Informationen finden Sie unter „Dateiübertragungsereignisse auf dem Controller und auf dem Zielrechner protokollieren" auf Seite 118.

Kapitel 12. Fehlerbehebung und Leistungsoptimierung

Im ersten Teil dieses Anhangs, „Fehlerbehebung", erhalten Sie einen Überblick über die Tasks, die Sie ausführen müssen, um die Informationen zu sammeln, die Sie zur Lösung von Problemen mit Tivoli Remote Control benötigen. Außerdem enthält er eine Beschreibung der gesammelten Informationen.

Im zweiten Teil dieses Anhangs, „Leistung steigern" auf Seite 133, werden Möglichkeiten zur Verbesserung der Leistung von Tivoli Remote Control beschrieben.

Fehlerbehebung

Um einen Fehler in Tivoli Remote Control zu beheben, sammeln Sie folgende Informationen und senden Sie sie an die Kundenunterstützung:

- Tivoli Remote Control-Protokolle
- Tivoli Remote Control-Traces
- Tivoli Remote Control-Anwendungsereignisse
- Tivoli-Server-Traces
- Endpunktprotokoll
- Umgebungsinformationen

Welche Informationen Sie angeben müssen, hängt von der Umgebung und der Art des Problems ab, das aufgetreten ist. Wenden Sie sich an die Kundenunterstützung, um zu erfahren, welche Informationen Sie sammeln sollen. In den folgenden Abschnitten erfahren Sie, wie Sie die Informationen zur Fehlerbehebung generieren können:

- „Tivoli Remote Control-Protokolle festlegen"
- „Tivoli Remote Control-Traces festlegen" auf Seite 121
- „Anwendungsereignisse auf einem Windows NT-, Windows 2000- oder Windows XP-Controller protokollieren" auf Seite 130
- „Tivoli-Server-Traces festlegen" auf Seite 132
- „Endpunktfehler protokollieren" auf Seite 132
- „Umgebungsinformationen sammeln" auf Seite 132

Tivoli Remote Control-Protokolle festlegen

Sie können, wie in den folgenden Abschnitten beschrieben, Protokolldateien generieren, die Tivoli Remote Control-Sitzungsereignisse oder Installationsinformationen enthalten:

Remote Control-Ereignisse auf dem Controller und auf dem Zielrechner protokollieren

Auf Windows-Plattformen können Sie die Protokollierung von Remote Control-Ereignissen oder Fehlern aktivieren, die während einer Sitzung auftreten, indem Sie die Schlüsselwörter im Abschnitt LOGGING der Datei `Windows-Installationsverzeichnis\remcon.ini` des Controllers und der Zielworkstations festlegen:

```
[LOGGING]
log_level=1
log_size=1000000
```

Dabei gilt:

log_level
Aktiviert die Protokollstufe und legt sie fest. Mögliche Werte:
1 Es werden nur Fehlernachrichten protokolliert.
2 Es werden Fehlernachrichten und Warnungen protokolliert.
3 Es werden Fehlernachrichten, Warnungen und informative Nachrichten protokolliert.

Der Standardwert beträgt 1.

log_size
Gibt die maximale Größe der Protokolldatei an. Der Standardwert beträgt 1.000.000 Bytes. Wenn diese Datei eine Größe von 1.000.000 Bytes erreicht, wird ihr Inhalt in eine BAK-Datei verschoben, die ebenfalls über eine Kapazität von 1.000.000 Bytes verfügt.Die folgenden Ereignisse werden weiter in der Protokolldatei festgehalten, bis sie die genannte Größe erreicht. Anschließend wird das Sicherungsverfahren wiederholt.

Folgende Protokolldateien werden unter Windows erstellt:

- *<lcf>*\PCREMOTE*<i>*\CTL\Logs\remcon.log auf dem Controller
  Dabei gilt:

  <*lcf*> ist das Installationsverzeichnis des Tivoli-Managementagenten.

  <*i*> kann einen der folgenden Werte annehmen:
  – 'w32-ix86' für Windows NT, Windows 2000 und Windows XP
  – 'win95' für Windows 98 Second Edition
- *<lcf>*\PCREMOTE*<i>*\TGT\Logs\remcon.log auf dem Zielrechner. Diese Datei wird auf Windows 98 Second Edition-Zielrechnern nicht erstellt.

Auf OS/2-Plattformen werden die folgenden Protokolldateien immer erstellt. Sie enthalten die Fehlernachrichten und die Informationen zum Sitzungsende:

- *<lcf>*\PCREMOTE\os2-ix86\CTL\eqnmgr.log auf dem Controller
  Dabei gilt:

  <*lcf*> ist das Installationsverzeichnis des Tivoli-Managementagenten.
- *<lcf>*\PCREMOTE*<i>*\TGT\eqntg.log auf dem Zielrechner.

Dateiübertragungsereignisse auf dem Controller und auf dem Zielrechner protokollieren

Die Protokollierung der Dateiübertragungsereignisse wird automatisch aktiviert. Auf dem Controller können Sie die Protokollstufe zur Laufzeit anpassen, indem Sie F2 drücken. Wenn Sie eine neue Sitzung starten, wird der Wert der Protokollstufe mit dem Standardwert überschrieben.

Sie können einen neuen Standardwert definieren, indem Sie folgende Dateien erstellen:

- *<lcf>*\PCREMOTE*<i>*\CTL\ft_ctl.cfg auf dem Controller
  Dabei gilt:

  <*lcf*> ist das Installationsverzeichnis des Tivoli-Managementagenten.

  <*i*> kann einen der folgenden Werte annehmen:
  – 'w32-ix86' für Windows NT, Windows 2000 und Windows XP
  – 'win95' für Windows 98 Second Edition
  – 'os2-ix86' für OS/2

- <*lcf*>\PCREMOTE\<*i*>\TGT \ft_tgt.cfg auf dem Zielrechner

Die Dateien 'ft_ctl.cfg' und 'ft_tgt.cfg' müssen folgende Zeile enthalten:
`tmeLogger.msg.level=`*`Protokollstufe`*

Dabei gilt:

Protokollstufe Aktiviert die Protokollstufe und legt sie fest. Mögliche Werte:

OFF	Es wird keine Nachricht protokolliert.
INFO	Es werden nur informative Nachrichten protokolliert.
WARN	Es werden informative Nachrichten und Warnungen protokolliert.
ERROR	Es werden informative Nachrichten, Warnungen und Fehlernachrichten protokolliert.

Folgende Protokolldateien werden erstellt:

- <*lcf*>\PCREMOTE\<*i*>\CTL\Logs\RCCTL_FT*JJJJMMTT@hhmmss*.log auf dem Controller.

  Dabei gilt:

<*lcf*>	ist das Installationsverzeichnis des Tivoli-Managementagenten.
<*i*>	kann einen der folgenden Werte annehmen: – 'w32-ix86' für Windows NT, Windows 2000 oder Windows XP – 'win95' für Windows 98 Second Edition – 'os2-ix86' für OS/2
JJJJMMTT	steht für das Jahr (4 Ziffern), den Monat (2 Ziffern) und den Tag (2 Ziffern). Beispiel: 20021105.
hhmmss	steht für die Stunden (2 Ziffern), Minuten (2 Ziffern) und Sekunden (2 Ziffern). Beispiel: 153350.

- <*lcf*>\PCREMOTE\<*i*>\TGT\Logs\RCTGT_FT.log auf dem Zielrechner.

Anmerkungen:

1. Damit lokalisierte DBCS-Zeichen korrekt angezeigt werden, müssen die Protokolldateien mit einer UTF-8-Anzeigefunktion geöffnet werden.
2. Bei FAT-Betriebssystemen haben die Protokolldateien zur Dateiübertragung folgendes Format: FT*xxxxxx*.log, wobei *xxxxxx* für eine fortlaufende Zahl steht.

Chat-Ereignisse auf dem Controller und auf dem Zielrechner protokollieren

Die Protokollierung der Chat-Ereignisse wird automatisch aktiviert. Sie können die Protokollstufe zur Laufzeit anpassen, indem Sie F2 drücken. Wenn Sie eine neue Sitzung starten, wird der Wert der Protokollstufe mit dem Standardwert überschrieben.

Sie können einen neuen Standardwert definieren, indem Sie folgende Dateien erstellen:

- <*lcf*>\PCREMOTE\<*i*>\CTL\ch_ctl.cfg auf dem Controller

  Dabei gilt:

<*lcf*>	ist das Installationsverzeichnis des Tivoli-Managementagenten.
<*i*>	kann einen der folgenden Werte annehmen:

  - 'w32-ix86' für Windows NT, Windows 2000 und Windows XP
  - 'win95' für Windows 98 Second Edition
  - 'os2-ix86' für OS/2
- <*lcf*>\PCREMOTE\<*i*>\TGT\ch_tgt.cfg auf dem Zielrechner

Die Dateien 'ch_ctl.cfg' und 'ch_tgt.cfg' müssen folgende Zeile enthalten:

`tmeLogger.msg.level=`*`Protokollstufe`*

Dabei gilt:

Protokollstufe Aktiviert die Protokollstufe und legt sie fest. Mögliche Werte:

OFF	Es wird keine Nachricht protokolliert.
INFO	Es werden nur informative Nachrichten protokolliert.
WARN	Es werden informative Nachrichten und Warnungen protokolliert.
ERROR	Es werden informative Nachrichten, Warnungen und Fehlernachrichten protokolliert.

Folgende Protokolldateien werden erstellt:

- <*lcf*>\PCREMOTE\<*i*>\CTL\Logs\RCCTL_CH*JJJJMMTT@hhmmss*.log auf dem Controller

  Dabei gilt:

<*lcf*>	ist das Installationsverzeichnis des Tivoli-Managementagenten.
<*i*>	kann einen der folgenden Werte annehmen: – 'w32-ix86' für Windows NT, Windows 2000 oder Windows XP – 'win95' für Windows 98 Second Edition – 'os2-ix86' für OS/2
JJJJMMTT	steht für das Jahr (4 Ziffern), den Monat (2 Ziffern) und den Tag (2 Ziffern). Beispiel: 20021105.
hhmmss	steht für die Stunden (2 Ziffern), Minuten (2 Ziffern) und Sekunden (2 Ziffern). Beispiel: 153350.

- <*lcf*>\PCREMOTE\<*i*>\TGT\Logs\RCTGT_CH*JJJJMMTT@hhmmss*.log auf dem Zielrechner.

Anmerkungen:

1. Damit lokalisierte DBCS-Zeichen korrekt angezeigt werden, müssen die Protokolldateien mit einer UTF-8-Anzeigefunktion geöffnet werden.
2. Bei FAT-Betriebssystemen haben die Chat-Protokolldateien folgendes Format: CH*xxxxxx*.log, wobei *xxxxxx* für eine fortlaufende Zahl steht.

Inhalt der Protokolldateien

Jeder Eintrag in den Protokolldateien enthält folgende Daten:

Datum_Uhrzeit Fernes_System Lokales_System Nachrichtencode Nachrichtentext

Dabei gelten die folgenden Definitionen:

Datum_Uhrzeit Datum und Uhrzeit, zu der die Nachricht geschrieben wurde.

Fernes_System Hostname der fernen Workstation.

Lokales_System Hostname der lokalen Workstation, auf der die Protokolldatei gespeichert ist.

Nachrichtencode
Nachrichtencode.

Nachrichtentext Text der Nachricht.

Installationsinformationen auf dem Remote Control-Server protokollieren

Wenn Sie mit dem Befehl **wrcinstep** Controller- und Zielrechnerkomponenten installieren und die Installation fehlschlägt, wird folgende Protokolldatei generiert:

- Unter Windows 2000:

  `\temp\rctrace\RCL_wrcinstep.log`
- Unter UNIX, Linux für Intel und Linux für S/390:

  `/tmp/rctrace/RCL_wrcinstep.log`

Tivoli Remote Control-Traces festlegen

Sie können für Tivoli Remote Control-Server, -Controller und -Zielrechner wie in den folgenden Abschnitten beschrieben Traces festlegen:

- „Traces auf dem Remote Control-Server festlegen"
- „Traces auf einem Windows-Controller und -Zielrechner festlegen" auf Seite 122
- „Traces auf einem OS/2-Controller und -Zielrechner festlegen" auf Seite 127

Traces auf dem Remote Control-Server festlegen

Um in Tivoli Remote Control Traces zu aktivieren oder zu inaktivieren oder die Tracestufe zu ändern, muss folgende Anweisung editiert werden:

```
NO 6
```

und zwar in der folgenden Datei:

- Unter Windows 2000:

  `\temp\rctrace\trace.cfg`
- Unter UNIX, Linux für Intel und Linux für S/390:

  `/tmp/rctrace/trace.cfg`

Der erste Wert kann entweder **NO** sein, um Traces zu inaktivieren oder **YES**, um Traces zu aktivieren.

Der zweite Wert steht für die Protokollstufe, die Sie in der Datei `trace.cfg` festlegen können:

3 Es werden Hauptaufrufe protokolliert.
4 Es werden Hauptmethoden protokolliert.
5 Es werden Methoden und Aufrufe protokolliert.
6 Es wird alles protokolliert.

Anmerkung: Die Datei 'trace.cfg' wird erstellt, wenn Sie zum ersten Mal auf das Symbol für Tivoli Remote Control klicken.

Die Tracedatei wird im folgenden Verzeichnis erstellt:

- Unter Windows 2000:

  `\temp\rctrace`

- Unter UNIX, Linux für Intel und Linux für S/390:

  ```
  /tmp/rctrace
  ```

Der Name der Datei ist *MMTThhss*.**TRC**. Dabei gilt: *MM* steht für Monat, *TT* steht für Tag, *hh* steht für Stunde, *ss* steht für Minute.

Traces auf einem Windows-Controller und -Zielrechner festlegen

Unter Windows können Sie folgende Tracearten aktivieren:

- Remote Control-Traces. Siehe „Remote Control-Traces (nicht gültig für Windows 98 Second Edition-Zielrechner)".
- Dateiübertragungs- und Chat-Traces. Siehe „Dateiübertragungstraces" auf Seite 124.

Remote Control-Traces (nicht gültig für Windows 98 Second Edition-Zielrechner): Um Traces für Tastaturinformationen, Kommunikationsinformationen oder andere Informationsarten zu aktivieren bzw. die Traceeinstellungen zu ändern, editieren Sie folgende Abschnitte der Datei `Windows-Installationsverzeichnis\remcon.ini` des Controllers und der Zielworkstations:

```
[GENERIC]
trace_level=0
trace_size=1000000
trace_length=64

[KEYBOARD]
trace_level=0
trace_size=1000000
trace_length=64

[FILTER]
trace_level=0
trace_size=1000000
trace_length=64

[COMMUNICATION]
trace_level=0
trace_size=1000000
trace_length=64

[LOGON]
trace_level=0
trace_size=1000000
trace_length=64

[WTS]
trace_level=0
trace_size=1000000
trace_length=64

[START]
trace_level=0
trace_size=1000000
trace_length=64

[GRAPHICENGINE]
trace_level=0
trace_size=1000000
trace_length=64

[TERMINATION]
trace_level=0
trace_size=1000000
trace_length=64
```

```
[DESKTOPOPTIMIZATION]
trace_level=0
trace_size=1000000
trace_length=64
```

Dabei gilt:

trace_level

Aktiviert die Traces und legt die Tracestufe fest. Mögliche Werte:

0 Es wird kein Trace durchgeführt.

1 Es wird nur für Fehlernachrichten ein Trace durchgeführt.

2 Es wird für Fehlernachrichten und Warnungen ein Trace durchgeführt.

3 Es wird für Fehlernachrichten, Warnungen und informative Nachrichten ein Trace durchgeführt.

Der Standardwert beträgt 0.

trace_size

Gibt die maximale Größe der Tracedatei an. Der Standardwert beträgt 1.000.000 Bytes. Wenn die Größe der Tracedatei überschritten wird, wird eine BAK-Datei erstellt. Die folgenden Ereignisse werden weiter in der Tracedatei festgehalten, bis sie die genannte Größe erreicht. Anschließend wird das Sicherungsverfahren wiederholt.

trace_length

Gibt an, für wie viele Bytes ein Trace durchgeführt werden soll. Der Standardwert beträgt 64.

Je nach editiertem Abschnitt werden unterschiedliche Tracedateien generiert:

Tabelle 1.

Abschnitt	Bedeutung des Abschnitts	Tracedateiname
[GENERIC]	Führt ein Trace für allgemeine Informationen durch	remcon.trc
[KEYBOARD]	Führt ein Trace für Tastaturinformationen durch	keyboard.trc
[FILTER]	Führt ein Trace für Filterinformationen durch	filter.trc
[COMMUNICATION]	Führt ein Trace für Kommunikationsinformationen durch	sndrcv.trc
[WTS]	Führt ein Trace für Terminal Server-Informationen durch	wts.trc
[LOGON]	Führt ein Trace für Anmeldeinformationen durch	logon.trc
[START]	Führt ein Trace für die Vorgänge durch, mit denen eine Sitzung gestartet wird	start.trc
[GRAPHICENGINE]	Führt ein Trace für die Funktionen durch, mit denen grafische Vorgänge ausgeführt werden	graphicengine.trc
[SESSIONTERMINATION]	Führt ein Trace für die Vorgänge durch, mit denen eine Sitzung beendet wird	sessiontermination.trc

Tabelle 1. (Forts.)

Abschnitt	Bedeutung des Abschnitts	Tracedateiname
[DESKTOPOPTIMIZATION]	Führt ein Trace für die Funktionen zur Desktopoptimierung, z. B. Inaktivierung des Hintergrunds, durch	desktopoptimization.trc

Die Tracedateien werden in den folgenden Verzeichnissen erstellt:
- <*lcf*>\PCREMOTE\<*i*>\CTL\Trace auf dem Controller
- <*lcf*>\PCREMOTE\<*i*>\TGT\Trace auf dem Zielrechner

Dabei gilt:

<*lcf*> ist das Installationsverzeichnis des Tivoli-Managementagenten.

<*i*> kann einen der folgenden Werte annehmen:
- 'w32-ix86' für Windows NT, Windows 2000 oder Windows XP
- 'win95' für Windows 98 Second Edition (nur für den Controller gültig)

Remote Control-Traces auf Windows 98 Second Edition-Zielrechner: Um auf einem Windows 98-Zielrechner Remote Control-Traces zu aktivieren oder zu inaktivieren oder die Tracestufe zu ändern, muss der Wert für die **Tracelänge** des folgenden Registrierungsschlüssels im Registrierungseditor **regedit** bzw. regedt32 editiert werden.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Remote Control Target
```

Der Wert für die **Tracelänge** zeigt an, wie viele Bytes für jeden Kommunikationspuffer verfolgt werden sollen. Der empfohlene Wert ist **40**. Der Standardwert **0** bedeutet, dass es keinen Trace gibt.

Die Tracedatei wird im Verzeichnis <*LCF_Verz*>\PCREMOTE\win95\TGT erstellt, wobei <*LCF_Verz*> das Verzeichnis ist, in dem der Tivoli-Managementagent installiert wurde.

Der Name der Tracedatei ist <*lcf*>\PCREMOTE\win95\TGT\Trace*MMTThhss*.TRC. Dabei gilt: *MM* steht für Monat, *TT* steht für Tag, *hh* steht für Stunde und *ss* steht für Minute.

Dateiübertragungstraces: Die Dateiübertragungstraces werden automatisch aktiviert. Sie können auf dem Controller die Tracestufe zur Laufzeit festlegen, indem Sie F3 drücken. Wenn Sie eine neue Sitzung starten, wird der Wert der Tracestufe mit dem Standardwert überschrieben.

Sie können einen neuen Standardwert definieren, indem Sie folgende Dateien erstellen:
- <*lcf*>\PCREMOTE\<*i*>\CTL\ft_ctl.cfg auf dem Controller

  Dabei gilt:

  <*lcf*> ist das Installationsverzeichnis des Tivoli-Managementagenten.

  <*i*> kann einen der folgenden Werte annehmen:
  - 'w32-ix86' für Windows NT, Windows 2000 und Windows XP
  - 'win95' für Windows 98 Second Edition
  - 'os2-ix86' für OS/2

- <*lcf*>\PCREMOTE\<*i*>\TGT\ft_tgt.cfg auf dem Zielrechner
  Die Dateien 'ft_ctl.cfg' und 'ft_tgt.cfg' müssen folgende Zeile enthalten:
  `tmeLogger.trc.level=`*`Tracestufe`*

  Dabei gilt:

  Tracestufe Aktiviert die Tracestufe und legt sie fest. Mögliche Werte:

OFF	Es wird kein Trace durchgeführt.
DEBUG_MIN	Es wird nur für Fehlernachrichten ein Trace durchgeführt.
DEBUG_MID	Es wird für Fehlernachrichten und Warnungen ein Trace durchgeführt.
DEBUG_MAX	Es wird für Fehlernachrichten, Warnungen und informative Nachrichten ein Trace durchgeführt.

  Folgende Tracedateien werden erstellt:
  – <*lcf*>\PCREMOTE\<*i*>\CTL\Logs\RCCTL_FT*JJJJMMTT@hhmmss*.log auf dem Controller.
    Dabei gilt:

<*lcf*>	ist das Installationsverzeichnis des Tivoli-Managementagenten.
<*i*>	kann einen der folgenden Werte annehmen: - 'w32-ix86' für Windows NT, Windows 2000 oder Windows XP - 'win95' für Windows 98 Second Edition - 'os2-ix86' für OS/2
JJJJMMTT	steht für das Jahr (4 Ziffern), den Monat (2 Ziffern) und den Tag (2 Ziffern). Beispiel: 20021105.
hhmmss	steht für die Stunden (2 Ziffern), Minuten (2 Ziffern) und Sekunden (2 Ziffern). Beispiel: 153350.

  – <*lcf*>\PCREMOTE\<*i*>\TGT\Logs\RCTGT_FT.log auf dem Zielrechner.

  Folgende Tracedateien werden erstellt:
  – <*lcf*>\PCREMOTE\<*i*>\CTL\Trace\RCCTL_FT*JJJJMMTT@hhmmss*.trc auf dem Controller.
    Dabei gilt:

<*lcf*>	ist das Installationsverzeichnis des Tivoli-Managementagenten.
<*i*>	kann einen der folgenden Werte annehmen: - 'w32-ix86' für Windows NT, Windows 2000 oder Windows XP - 'win95' für Windows 98 Second Edition - 'os2-ix86' für OS/2
JJJJMMTT	steht für das Jahr (4 Ziffern), den Monat (2 Ziffern) und den Tag (2 Ziffern). Beispiel: 20021105.

hhmmss steht für die Stunden (2 Ziffern), Minuten (2 Ziffern) und Sekunden (2 Ziffern). Beispiel: 153334.

– <*lcf*>\PCREMOTE\<i>\TGT\Trace\RCTGT_FT.trc auf dem Zielrechner

Anmerkungen:

1. Damit lokalisierte DBCS-Zeichen korrekt angezeigt werden, müssen die Tracedateien mit einer UTF-8-Anzeigefunktion geöffnet werden.
2. Bei FAT-Betriebssystemen haben die Tracedateien zur Dateiübertragung folgendes Format: FT*xxxxxx*.trc, wobei *xxxxxx* für eine fortlaufende Zahl steht.

Chat-Traces: Die Chat-Traces werden automatisch aktiviert. Sie können die Tracestufe zur Laufzeit anpassen, indem Sie F3 drücken. Wenn Sie eine neue Sitzung starten, wird der Wert der Tracestufe mit dem Standardwert überschrieben.

Sie können einen neuen Standardwert definieren, indem Sie folgende Dateien erstellen:

- <*lcf*>\PCREMOTE\<*i*>\CTL\ch_ctl.cfg auf dem Controller

  Dabei gilt:

  <*lcf*> ist das Installationsverzeichnis des Tivoli-Managementagenten.

  <*i*> kann einen der folgenden Werte annehmen:
  – 'w32-ix86' für Windows NT, Windows 2000 und Windows XP
  – 'win95' für Windows 98 Second Edition
  – 'os2-ix86' für OS/2

- <*lcf*>\PCREMOTE\<*i*>\TGT\ch_tgt.cfg auf dem Zielrechner

  Die Dateien 'ch_ctl.cfg' und 'ch_tgt.cfg' müssen folgende Zeile enthalten:

  `tmeLogger.trc.level=`*`Tracestufe`*

  Dabei gilt:

  Tracestufe Aktiviert die Tracestufe und legt sie fest. Mögliche Werte:

OFF	Es wird kein Trace durchgeführt.
DEBUG_MIN	Es wird nur für Fehlernachrichten ein Trace durchgeführt.
DEBUG_MID	Es wird für Fehlernachrichten und Warnungen ein Trace durchgeführt.
DEBUG_MAX	Es wird für Fehlernachrichten, Warnungen und informative Nachrichten ein Trace durchgeführt.

  Folgende Tracedateien werden erstellt:

  – <*lcf*>\PCREMOTE\<*i*>\CTL\Trace\RCCTL_CH*JJJJMMTT@hhmmss*.trc auf dem Controller

  Dabei gilt:

  <*lcf*> ist das Installationsverzeichnis des Tivoli-Managementagenten.

  <*i*> kann einen der folgenden Werte annehmen:
  - 'w32-ix86' für Windows NT, Windows 2000 oder Windows XP
  - 'win95' für Windows 98 Second Edition

- 'os2-ix86' für OS/2

JJJJMMTT steht für das Jahr (4 Ziffern), den Monat (2 Ziffern) und den Tag (2 Ziffern). Beispiel: 20021105.

hhmmss steht für die Stunden (2 Ziffern), Minuten (2 Ziffern) und Sekunden (2 Ziffern). Beispiel: 153350.

– <*lcf*>\PCREMOTE\<*i*>\TGT\Trace\RCTGT_CH*JJJJMMTT@hhmmss*.trc auf dem Zielrechner

Anmerkungen:

1. Damit lokalisierte DBCS-Zeichen korrekt angezeigt werden, müssen die Tracedateien mit einer UTF-8-Anzeigefunktion geöffnet werden.
2. Bei FAT-Betriebssystemen haben die Chat-Tracedateien folgendes Format: CH*xxxxxx*.trc, wobei *xxxxxx* für eine fortlaufende Zahl steht.

Traces auf einem OS/2-Controller und -Zielrechner festlegen

Um einen Trace auf einem OS/2-Controller oder -Zielrechner festzulegen, ist der Datei **CONFIG.SYS** folgende Anweisung hinzuzufügen:

```
SET RCDEBUG=xxyy
```

Dabei kann *xxyy* die folgenden Werte annehmen:

Ereignis	Wert	Anmerkungen
Tivoli Remote Control	0100	Die Ereignisse werden in einer Datei protokolliert.
TCP/IP	02*yy*	*yy* gibt die Anzahl der Bytes an, die für jedes Senden oder Empfangen in der Tracedatei gespeichert werden soll. Der Höchstwert beträgt 99. Der empfohlene Wert ist 40.

Um weitere Arten von Ereignissen verfolgen zu können, muss *xxxx* als Summe der Einzelwerte definiert werden.

Um beispielsweise Traces für das TCP/IP-Protokoll und Tivoli Remote Control-Ereignis zu aktivieren, fügen Sie der Datei **CONFIG.SYS** folgendes hinzu:

```
SET RCDEBUG=0340
```

Dabei ist *0340* die Summe von:

- *0100* (Wert des Tivoli Remote Control-Ereignisses)
- *0200* (Wert des TCP/IP-Ereignisses)
- *40* (Anzahl der für die TCP/IP-Kommunikation zu speichernden Bytes).

Anmerkung: Nachdem Sie die oben aufgeführte Anweisung der Datei **CONFIG-.SYS** hinzugefügt haben, starten Sie die Maschine neu, um die Änderungen in den Speicher zu übernehmen.

Inhalt der Tracedatei

Jeder Eintrag in den Tracedateien enthält folgende Daten:

Datum_Uhrzeit Fernes_System Lokales_System Nachrichtentext

Dabei gelten die folgenden Definitionen:

Datum_Uhrzeit Datum und Uhrzeit, zu der die Nachricht geschrieben wurde.

Fernes_System Hostname der fernen Workstation.

Lokales_System Hostname der lokalen Workstation, auf der die Tracedatei gespeichert ist.

Nachrichtentext Text der Nachricht.

Anmerkung: Wenn Sie OS/2 als Betriebssystem oder den Abschnitt COMMUNICATION verwenden, ist der *Nachrichtentext* ein Übertragungspuffer. Dieser kann Folgendes enthalten:

- Die bei einer Sende- oder Empfangsoperation gesendeten oder empfangenen Daten. Die Anzahl der gespeicherten Bytes hängt vom Wert in der Variablen **Trace Length** (Tracelänge) ab. - oder -
- Eine Zeichenfolge, die anzeigt, ob eine Verbindungs- oder Schließoperation ausgeführt wurde.

Zusammenfassung der Tivoli Remote Control-Protokolle und -Traces

In der folgenden Tabelle sind die Tivoli Remote Control-Protokolle und -Traces aufgeführt, die unter UNIX, Linux für Intel, Linux für S/390, Windows und OS/2 verfügbar sind. Wie sie erstellt werden, erfahren Sie in folgenden Abschnitten:

- „Remote Control-Ereignisse auf dem Controller und auf dem Zielrechner protokollieren" auf Seite 117.
- „Traces auf dem Remote Control-Server festlegen" auf Seite 121.
- „Traces auf einem Windows-Controller und -Zielrechner festlegen" auf Seite 122.
- „Traces auf einem OS/2-Controller und -Zielrechner festlegen" auf Seite 127.

Protokolle und Traces für	**UNIX, Linux für Intel, Linux für S/390**		
	Pfad für Protokolle und Traces	**Tracenamen**	**Protokollnamen**
Remote Control-Server	/tmp/rctrace/	*MMTThhss*.trc (*)	
Befehl **wrcinstep**	/tmp/rctrace/		RCL_wrcinstep.log
Befehl **wrcuninstep**	/tmp/rctrace/		RCL_wrcuninstep.log

(*): Dabei gilt:

MMTThhss *MM* steht für den Monat, *TT* für den Tag, *hh* für die Stunden und *ss* für die Minuten

Protokolle für	**Windows**	
	Pfad für Protokolle	**Protokollnamen**
Remote Control-Controller	<*lcf*>\PCREMOTE\<*i*>\CTL\LOGS\ (*)	remcon.log
Remote Control-Zielrechner	<*lcf*>\PCREMOTE\<*i*>\TGT\LOGS\	remcon.log
Chat-Controller	<*lcf*>\PCREMOTE\<*i*>\CTL\Trace	RCCTL_CH*JJJJMMTT@hhmmss*.log
Chat-Zielrechner	<*lcf*>\PCREMOTE\<*i*>\TGT\Trace	RCTGT_CH*JJJJMMTT@hhmmss*.log
Controller für Dateiübertragung	<*lcf*>\PCREMOTE\<*i*>\CTL\Trace	RCCTL_FT*JJJJMMTT@hhmmss*.log
Zielrechner für Dateiübertragung	<*lcf*>\PCREMOTE\<*i*>\TGT\Trace	RCTGT_FT.log
Befehl **wrcinstep**	\temp\rctrace\	RCL_wrcinstep.log

Zusammenfassung der Tivoli Remote Control-Protokolle und -Traces

Traces für	**Windows**	
	Pfad für Traces	**Tracenamen**
Remote Control-Server	\temp\rctrace\	*MMTThhss*.trc (*)
Allgemeine Informationen des Controllers	<*lcf*>\PCREMOTE\<*i*>\CTL\TRACE\ (*)	remcon.trc
Tastaturinformationen des Controllers	<*lcf*>\PCREMOTE\<*i*>\CTL\TRACE\ (*)	keyboard.trc
Informationen zum Sitzungsstart des Controllers	<*lcf*>\PCREMOTE\<*i*>\CTL\TRACE\ (*)	start.trc
Übertragungsinformationen des Controllers	<*lcf*>\PCREMOTE\<*i*>\CTL\TRACE\ (*)	sndrcv.trc
Informationen zum Sitzungsende des Controllers	<*lcf*>\PCREMOTE\<*i*>\CTL\TRACE\ (*)	termination.trc
Terminal Server-Informationen des Controllers	<*lcf*>\PCREMOTE\<*i*>\CTL\TRACE\ (*)	wts.trc
Allgemeine Informationen des Zielrechners	<*lcf*>\PCREMOTE\w32-ix86\TGT\TRACE\ (*)	remcon.trc
Tastaturinformationen des Zielrechners	<*lcf*>\PCREMOTE\w32-ix86\TGT\TRACE\ (*)	keyboard.trc
Anmeldeinformationen des Zielrechners	<*lcf*>\PCREMOTE\w32-ix86\TGT\TRACE\ (*)	logon.trc
Informationen zum Sitzungsstart des Zielrechners	<*lcf*>\PCREMOTE\w32-ix86\TGT\TRACE\ (*)	start.trc
Übertragungsinformationen des Zielrechners	<*lcf*>\PCREMOTE\w32-ix86\TGT\TRACE\ (*)	sndrcv.trc
Informationen zur grafischen Steuerkomponente des Zielrechners	<*lcf*>\PCREMOTE\w32-ix86\TGT\TRACE\ (*)	graphicengine.trc
Informationen zum Sitzungsende des Zielrechners	<*lcf*>\PCREMOTE\w32-ix86\TGT\TRACE\ (*)	termination.trc
Informationen zur Desktopoptimierung des Zielrechners	<*lcf*>\PCREMOTE\w32-ix86\TGT\TRACE\ (*)	desktopoptimization.trc
Windows 98-Remote Control-Zielrechner	<*lcf*>\PCREMOTE\win95\TGT\TRACE\ (*)	*MMTThhss*.trc
Controller für Dateiübertragung	<*lcf*>\PCREMOTE\<*i*>\CTL\Trace (*)	RCCTL_FT*JJJJMMTT@hhmmss*.trc
Zielrechner für Dateiübertragung	<*lcf*>\PCREMOTE\<*i*>\TGT\Trace (*)	RCTGT_FT.trc
Chat-Controller	<*lcf*>\PCREMOTE\<*i*>\CTL\Trace (*)	RCCTL_CH*JJJJMMTT@hhmmss*.trc
Chat-Zielrechner	<*lcf*>\PCREMOTE\<*i*>\TGT\Trace (*)	RCTGT_CH*JJJJMMTT@hhmmss*.trc

(*): Dabei gilt:

<*lcf*> ist das Installationsverzeichnis des Tivoli-Managementagenten.

<*i*> kann einen der folgenden Werte annehmen:
- **w32-ix86** für Windows NT-, Windows 2000- oder Windows XP-Controller und -Zielrechner

- **win95** für Windows 98 Second Edition

MMTThhss steht für den Monat (2 Ziffern), den Tag (2 Ziffern), die Stunden (2 Ziffern) und die Minuten (2 Ziffern). Beispiel: 11051533.

JJJJMMTT steht für das Jahr (4 Ziffern), den Monat (2 Ziffern) und den Tag (2 Ziffern). Beispiel: 20021105.

hhmmss steht für die Stunden (2 Ziffern), Minuten (2 Ziffern) und Sekunden (2 Ziffern). Beispiel: 153350.

Protokolle und Traces für	**OS/2**		
	Pfad für Protokolle und Traces	**Tracenamen**	**Protokollnamen**
Remote Control-Controller	<*lcf*>\PCREMOTE\<i>\CTL\TRACE\	*MMTThhss*.TRC (*)	
	<*lcf*>\PCREMOTE\<i>\CTL\	EQN02TC.TRC	EQNMGR.log
Remote Control-Zielrechner	<*lcf*>\PCREMOTE\<i>\TGT\TRACE\	*MMTThhss*.TRC	
	<*lcf*>\PCREMOTE\<i>\TGT\	EQN02TC.TRC	EQNTG.log
Controller für Dateiübertragung	<*lcf*>\PCREMOTE\<i>\CTL\Trace	RCCTL_FT*JJJJMMTT@hhmmss*.TRC	RCCTL_FT*JJJJMMTT@hhmmss*.log
Zielrechner für Dateiübertragung	<*lcf*>\PCREMOTE\<i>\TGT\Trace	RCTGT_FT.TRC	RCTGT_FT.log
Chat-Controller	<*lcf*>\PCREMOTE\<i>\CTL\Trace	RCCTL_CH*JJJJMMTT@hhmmss*.TRC	RCCTL_CH*JJJJMMTT@hhmmss*.log
Chat-Zielrechner	<*lcf*>\PCREMOTE\<i>\TGT\Trace	RCTGT_CH*JJJJMMTT@hhmmss*.TRC	RCTGT_CH*JJJJMMTT@hhmmss*.log

Dabei gilt:

<*lcf*> ist das Installationsverzeichnis des Tivoli-Managementagenten.

<*i*> steht für 'os2-ix86'.

MMTThhss steht für den Monat (2 Ziffern), den Tag (2 Ziffern), die Stunden (2 Ziffern) und die Minuten (2 Ziffern). Beispiel: 11051533.

JJJJMMTT steht für das Jahr (4 Ziffern), den Monat (2 Ziffern) und den Tag (2 Ziffern). Beispiel: 20021105.

hhmmss steht für die Stunden (2 Ziffern), Minuten (2 Ziffern) und Sekunden (2 Ziffern). Beispiel: 153350.

Anwendungsereignisse auf einem Windows NT-, Windows 2000- oder Windows XP-Controller protokollieren

In der Ereignisanzeige eines Windows NT-, Windows 2000- oder Windows XP-Controllers können fünf Tivoli Remote Control-Ereignisse protokolliert werden, indem der Protokollierungswert eines Registrierungsschlüssels mit dem Programm **regedit** festgelegt wird. Dazu gehören folgende fünf Ereignisse:

- <*Controller-Hostname*> `taking over` <*Zielrechnername*>
- <*Controller-Hostname*> `closing session with` <Zielrechnername>
- <*Controller-Hostname*> `could not establish session with` <Zielrechnername>. Error: <*Fehler*>
- <*Controller-Hostname*> `startup error` <*Fehler*>

- <*Controller-Hostname*> `closing session with` <*Zielrechnername*>. Error: <*Fehler*>

Um diese Ereignisse zu protokollieren, muss der Wert für **Logging** des folgenden Registrierungsschlüssels editiert werden:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Remote Control Controller
```

Gültige Einträge für **Logging** sind:

0	Ereignisse werden nicht protokolliert
1	Ereignisse werden protokolliert

Der Standardwert ist **0**.

Um Tivoli Remote Control-Ereignisse in der Ereignisanzeige des Terminal Servers zu protokollieren, legen Sie im folgenden Registrierungsschlüssel für den Benutzer, der über die Terminal Service-Sitzung angemeldet ist, die vollständige Berechtigung fest:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\
Tivoli Remote Control
```

Tivoli Enterprise Console verwenden

Wenn der TEC-Adapter (TEC - Tivoli Enterprise Console) installiert ist, können die protokollierten Ereignisse vom Controller aus angezeigt werden. Jedem Ereignis wird der Administratorname vorangestellt.

So zeigen Sie die protokollierten Ereignisse an:

1. Definieren Sie in der Datei **tecad_nt.conf** den TEC-Hostnamen.
2. Fügen Sie am Ende der Datei **tecad_nt.baroc** Folgendes hinzu:

```
TEC_CLASS:
   NT_RemoteControl_Event ISA NT_Base
   DEFINES {
       message: STRING;
            };
END
```

3. Fügen Sie am Ende der Datei **tecad_nt.fmt** Folgendes hinzu:

```
FORMAT NT_RemoteControl_Event FOLLOWS NT_Base
%t %s %s %s %s %s Remote Control %s %s*
message $8
END
```

4. Fügen Sie am Ende der Datei **tecad_nt.cds** Folgendes hinzu:

```
CLASS NT_RemoteControl_Event
  SELECT
    1: ATTR(=,"_event_id"), VALUE(=,"79");
    2: ATTR(=,"hostname");
    3: ATTR(=,"origin");
    4: ATTR(=,"category");
    5: ATTR(=,"eventType");
    6: ATTR(=,"sid");
    7: ATTR(=,"sub_source");
    8: ATTR(=,"id");
    9: ATTR(=,"msg");
    10: ATTR(=,"date1");
    11: ATTR(=,"date2");
    12: ATTR(=,"message");

MAP
  hostname = $V2;
  origin = $V3;
  category = $V4;
```

```
  eventType = $V5;
  sid = $V6;
  sub_source = $V7;
  id = $V8;
  msg = $V9;
  date= PRINTF("%s %s", $V10, $V11);
  message = $V12;
END
```

Weitere Informationen zu TEC finden Sie in den Handbüchern zu Tivoli Enterprise Console.

Tivoli-Server-Traces festlegen

Führen Sie folgende Schritte aus, um die Tivoli-Server-Tracedateien zu erstellen:

1. Führen Sie folgende Befehle aus:

   ```
   odadmin trace off
   odadmin trace errors
   odadmin trace objcalls
   odadmin trace services
   objcall 0.0.0 START TRACE
   ```

2. Reproduzieren Sie den Fehler.
3. Führen Sie folgende Befehle aus:

   Auf UNIX-, Linux für Intel- und Linux für S/390-Workstations

   ```
   objcall 0.0.0 STOP TRACE
   odstat > odstat.out
   odadmin db_sync
   wtrace -jHk $DBDIR > wtrace.out
   ```

   Auf Windows NT-, Windows 2000- und Windows XP-Workstations

   ```
   objcall 0.0.0 STOP TRACE
   odstat > odstat.out
   odadmin db_sync
   wtrace -jHk %DBDIR% > wtrace.out
   ```

Die Tracedateien `odstat.out` und `wtrace.out` werden im aktuellen Verzeichnis erstellt.

Endpunktfehler protokollieren

Führen Sie folgende Schritte aus, um Endpunktfehler zu protokollieren:

1. Legen Sie in der Datei 'last.cfg' auf dem Controller und auf dem Zielrechner den *Protokollschwellenwert* fest. Der Standardwert beträgt **1**. (Um weitere Informationen zu protokollieren, können Sie den Wert bis auf **4** erhöhen.)
2. Reproduzieren Sie den Fehler.

   Folgende Protokolldatei wird erstellt:

   `<`*lcf*`>\dat\<`*n*`>\lcfd.log`

   Dabei gilt:

   <*lcf*> ist das Installationsverzeichnis des Tivoli-Managementagenten.

   <*n*> ist die ganze Zahl, mit der die Verbindungsnummer des Endpunkts angegeben wird.

Umgebungsinformationen sammeln

Sie können Dateien generieren, die Hardware- und Softwareinformationen zur Workstation enthalten.

Workstation-Konfigurationsbericht

Führen Sie einen der folgenden Schritte aus, um einen Workstation-Konfigurationsbericht zu generieren:

- Führen Sie unter Windows NT, Windows 2000 und Windows XP folgenden Befehl über die Eingabeaufforderung aus:

  ```
  WINMSD /A
  ```

  Die Datei `<Hostname>.TXT` wird generiert.

- Wählen Sie unter Windows 98 Second Edition **Start → Programme → Zubehör → Systemprogramme → Systeminformationen** aus. Das Programm erfasst die Informationen zur Workstation, die Sie in einer Datei speichern können.

  Anmerkung: Um dieses Programm ausführen zu können, müssen Sie es möglicherweise zuerst von der Windows 98-CD installieren.

- Geben Sie unter OS/2 in der Befehlszeile Folgendes ein:

  ```
  syslevel > syslvl.out
  copy c:\config.sys copy_config.sys
  ```

  Sammeln Sie die Dateien `syslvl.out` und `copy_config.sys`, die im aktuellen Verzeichnis erstellt wurden.

Tastaturbelegungsprotokoll

Der Zielrechner generiert die Datei RCKEYBD.LOG in folgenden Zielverzeichnissen:

- Unter Windows NT, Windows 2000 und Windows XP im Verzeichnis `<drive>\WINNT\system32`.
- Unter Windows 98 Second Edition im Zielinstallationsverzeichnis.
- Unter OS/2 im Verzeichnis <lcf>/dat/<n>.

  Dabei gilt:

  <*lcf*> ist das Installationsverzeichnis des Tivoli-Managementagenten.

  <*n*> ist die ganze Zahl, mit der die Verbindungsnummer des Endpunkts angegeben wird.

Diese Datei enthält die Informationen zur Tastatur der Ziel- und Controller-Workstations.

Leistung steigern

Die Übertragungsverzögerung zwischen Zielrechner und Controller hängt von der Art der Verbindung zwischen den beiden Systemen sowie vom Betriebssystem des Zielrechners ab.

Wenn Zielrechner und Controller sich entweder in demselben LAN oder in verschiedenen LANs, die durch eine T1-Leitung verbunden sind, befinden, wird eine geringere Verzögerung erreicht.

Wenn Zielrechner und Controller sich jedoch in verschiedenen LANs befinden, die durch eine Leitung mit einer Übertragungsrate von 57,6 Kbyte/s (oder langsamer) verbunden sind, ist die Verzögerung größer. In diesem Fall können Sie die Leistung mit Hilfe des Parameters zur Leistungsoptimierung bei langsamen Verbindungen steigern, wenn der Zielrechner unter Windows NT, Windows 2000 oder Windows XP ausgeführt wird (siehe „rc_def_optimize" auf Seite 80).

Leistung steigern

Die Verzögerung kann durch eine Verkleinerung der zu übertragenden Datenmenge wie folgt ständig verringert werden:

- Inaktivieren Sie auf Windows-Zielrechnern bei Sitzungsbeginn den Bildschirmhintergrund (über 'rc_def_backgrnd'). Der Bildschirmhintergrund wird bei Sitzungsende wiederhergestellt.
- Aktivieren Sie die Komprimierung der übertragenen Daten.
- Legen Sie für die Aktualisierungsrate den Wert 50 fest (über 'rc_def_rate'). Wenn sich der Controller auf einem sehr langsamen Netzwerk befindet, während sich der Zielrechner auf einem LAN befindet, legen Sie für die Aktualisierungsrate einen höheren Wert fest. Je nach Übertragungsgeschwindigkeit des Netzwerk-Subsystems kann der Zielrechner den Wert für die Aktualisierungsrate auch automatisch ändern.
- Auf Windows NT-, Windows 2000- und Windows XP-Zielrechnern wurde eine neue Funktionzur Anzeigenerfassung (Screen Capture) hinzugefügt. Um ihn auf einem Windows NT-Zielrechner zu aktivieren, müssen Sie die Workstation nach der Installation neu starten.
- Auf Windows 98 Second Edition-Zielrechnern wurde eine neue Funktion zur Analyse von Images hinzugefügt. Auf Windows NT-, Windows 2000- und Windows XP-Zielrechnern, die den Parameter zur Leistungsoptimierung bei langsamen Verbindungen verwenden, ist dieselbe Funktion gültig. Um sie zu aktivieren, legen Sie als Anzahl der Farben, die beim Anzeigen des Zielbildschirms auf dem Controller verwendet werden, 16 oder 256 fest (über 'rc_def_color').
- Legen Sie für die **Farbpalette** des Controllers höchstens 65536 Farben fest.

Informationen zum Anpassen einiger dieser Kenndaten durch Festlegen der entsprechenden Werte für die Standardrichtlinienmethoden finden Sie unter „Sitzungseinstellungen anpassen" auf Seite 90.

In der folgenden Tabelle sind die Vorgänge zusammengefasst, die Sie ausführen können, um die Übertragungsverzögerung zwischen dem Zielrechner und dem Controller durch Reduzierung der übertragenen Datenmenge zu verringern.

Vorgänge zur Leistungssteigerung	**Windows**		**OS/2**
	NT/2000/XP	**98 Second Edition**	
Langsame Verbindung aktivieren (über 'rc_def_optimize')	✓		
Als Aktualisierungsrate 50 Millisekunden festlegen (über 'rc_def_rate')	✓	✓	✓
Bildschirmhintergrund des Zielrechners inaktivieren (über 'rc_def_backgrnd')	✓	✓	✓
Als Anzahl der Farben, die beim Anzeigen des Zielbildschirms auf dem Controller verwendet werden, 16 oder 256 festlegen (über 'rc_def_color')	✓	✓	✓ (*)
Für die Farbpalette des Controllers höchstens 65536 Farben festlegen	✓	✓	
Komprimierung aktivieren	✓	✓	✓

(*): Auf OS/2-Zielrechnern findet die Übertragung immer mit 16 Farben statt.

Sie können einige dieser Kenndaten anpassen, indem Sie die entsprechenden Werte für die Standardrichtlinienmethoden festlegen.

Zielrechner schnell in die Zielmaschinenliste laden

Um die Leistung zu steigern, wenn eine große Anzahl von Endpunkten in die Zielmaschinenliste des Remote Control-Fensters geladen wird, legen Sie einen der folgenden Werte fest:

- Für **rc_def_define** *UncheckedList*. Dadurch wird die Zielmaschinenliste aus der Richtlinienmethode geladen und ohne Überprüfung angezeigt.
- Für **rc_def_define** entweder *DefinableTargetList* oder *FilteredList* und für **rc_def_targets** *default-list*. Dadurch wird die Zielmaschinenliste aus der Tivoli Management Framework-Datenbank geladen und angezeigt. Wenn Sie für **rc_def_targets** andere Werte angeben, wird für jeden Zielrechnernamen, der in der Richtlinienmethode enthalten ist, eine Überprüfung durchgeführt, bevor er angezeigt wird.

Leistung steigern

Anhang A. Eingabehilfen

Die Funktionen der Eingabehilfe ermöglichen Benutzern mit körperlichen Behinderungen (z. B. mit eingeschränkter Beweglichkeit oder eingeschränktem Sehvermögen) die effektive Nutzung von Softwareprodukten. Die wichtigsten Funktionen der Eingabehilfe in diesem Produkt ermöglichen den Benutzern folgende Aktionen:

- Die Verwendung von Hilfstechnologie (z. B. die Software zur Bildschirmsprachausgabe und der digitale Sprachsynthesizer) zur akustischen Ausgabe des auf dem Bildschirm angezeigten Textes. Ausführliche Informationen zur Verwendung dieser Technologie in diesem Produkt finden Sie in der dazugehörigen Produktdokumentation.
- Den Aufruf spezifischer oder gleichgestellter Funktionen ausschließlich über die Tastatur.
- Die Vergrößerung der Bildschirmanzeige.

Darüber hinaus wurden die Eingabehilfefunktionen im Aufbau der Produktdokumentation wie folgt berücksichtigt:

- Die gesamte Dokumentation steht sowohl im HTML-Format als auch in konvertierbaren PDF-Formaten zur Verfügung, um die Nutzung der Bildschirmsprachausgabe zu optimieren.
- Für alle Bilder in der Dokumentation wird alternativ Text angezeigt, so dass Benutzer mit Sehschwächen den Inhalt der Bilder verstehen können.

In der Schnittstelle mit Hilfe der Tastatur navigieren

Im Produkt werden standardmäßige Tasten und Tastenkombinationen für Direktaufrufe verwendet und vom Betriebssystem angegeben. Weitere Informationen hierzu finden Sie in der Dokumentation zum Betriebssystem.

Vergrößerung der Bildschirmanzeige

Sie können die in den Produktfenstern angezeigten Informationen vergrößern, indem Sie die vom Betriebssystem, auf dem das Produkt ausgeführt wird, bereitgestellten Funktionen verwenden. In einer Microsoft Windows-Umgebung können Sie beispielsweise die Bildschirmauflösung verringern, um die Schriftgröße des auf dem Bildschirm angezeigten Textes zu erhöhen. Weitere Informationen hierzu finden Sie in der Dokumentation zum Betriebssystem.

Anhang B. Häufig gestellte Fragen

Im Folgenden finden Sie häufig gestellte Fragen, die Ihnen bei der Lösung eventuell auftretender Probleme in Tivoli Remote Control helfen sollen. Des weiteren finden Sie Anweisungen zum Umgehen von Problemen bzw. kürzere Lösungswege, die für die tägliche Arbeit hilfreich sind.

Installation

Was ist zu tun, wenn während der Installation eines Controllers oder Ziels auf einem Endpunkt etwas fehlschlägt?

Informationen hierzu finden Sie in folgender Datei: <*lcf*>\DAT\<*n*>\lcfd.log, wobei gilt: <lcf> ist das Installationsverzeichnis des Tivoli-Managementagenten und <n> ein ganzzahliger Wert, der die Endpunktverbindungsnummer angibt. Diese Datei enthält eine ausführliche Liste mit sämtlichen Ereignissen, die auf dem Endpunkt stattfinden.

Anmerkung: Wenn Sie weitere Fehlernachrichten anzeigen möchten, muss der Protokollierungsschwellenwert in der Datei `last.cfg` auf 3 oder 4 gesetzt und der Endpunkt anschließend neu gestartet werden. Alternativ dazu können Sie den Endpunkt über die Befehlszeile mit dem Parameter **-d** neu starten. Beispiel: **lcfd -d 3**: Mit diesem Befehl wird der Endpunkt neu gestartet und für den Parameter logging_threshold der Wert 3 festgelegt. Weitere Informationen zur Verwendung des Befehls **lcfd** finden Sie im Handbuch *Tivoli Framework Reference Manual*.

Warum wird das System nach erfolgter Installation der Zielrechner-Software nicht automatisch neu gestartet?

Es ist nicht immer wünschenswert, einen Zielrechner sofort neu zu starten, insbesondere, wenn der Benutzer gerade daran arbeitet. Mit Hilfe der Neustartfunktion kann ein sofortiger Neustart erreicht werden, oder Sie können auch -b verwenden, wenn Sie den Zielrechner mit Hilfe des Befehls **wrcinstep** installieren. Für die Neustartfunktion ist zwar der Tivoli-Managementagent notwendig, nicht aber die neuen Treiber.

Was ist zu tun, wenn nach der Installation der Programmkorrektur auf einem Gateway beim Starten einer Sitzung mit einem Endpunkt dieses Gateways die Fehlernachricht angezeigt wird, dass der Zugriff verweigert wird?

Überprüfen Sie, ob der Zielrechner sich bereits in einer Sitzung mit einem anderen Controller befindet. Wenn dies der Fall ist, müssen Sie warten, bis der Zielrechner zum Starten einer neuen Sitzung mit Ihrem Controller wieder verfügbar ist.

Steuern und Überwachen

Was ist zu tun, wenn während der Arbeit mit dem Controller- oder Zielrechner-endpunkt etwas fehlschlägt?

Sehen Sie in folgenden Dateien nach:

- Je nach ausgeführter Aktion in den Remote Control-, Dateiübertragungs- und Chat-Protokolldateien. Weitere Informationen finden Sie unter „Tivoli Remote Control-Protokolle festlegen" auf Seite 117.
- Je nach ausgeführter Aktion in den Remote Control-, Dateiübertragungs- und Chat-Tracedateien. Weitere Informationen finden Sie unter „Tivoli Remote Control-Traces festlegen" auf Seite 121.
- In der Datei <*lcf*>\DAT\<*n*>\lcfd.log, dabei gilt: <*lcf*> ist das Installationsverzeichnis des Tivoli-Managementagenten und <*n*> ein ganzzahliger Wert, der die Endpunktverbindungsnummer angibt. Diese Datei enthält eine ausführliche Liste mit sämtlichen Ereignissen, die auf dem Endpunkt stattfinden. Weitere Informationen finden Sie unter „Endpunktfehler protokollieren" auf Seite 132.

Selbst wenn ein Administrator über Berechtigungsklassen von Tivoli Remote Control-Ressourcen verfügt, kann er den Zielrechner-Endpunkt nicht steuern. Wieso?

Der Endpunkt muss in dem Richtlinienbereich definiert sein, in dem die Berechtigungsklassen von Tivoli Remote Control-Ressourcen festgelegt werden. Verwenden Sie den Befehl **wmv**, um einen Endpunkt in einem Richtlinienbereich zu definieren. Weitere Informationen zu diesen Befehlen finden Sie im Handbuch *Tivoli Framework Reference Manual*.

Nachdem Sie den Endpunkt dem Richtlinienbereich zugeordnet haben, müssen Sie das Tivoli-Gateway synchronisieren, an dem sich der Endpunkt anmeldet. Siehe „Schritt 4: Richtlinienbereichen Ziele zuordnen" auf Seite 70.

Die Sitzung mit einem Controller wurde soeben beendet. Kann er aktiviert und in einer Sitzung mit einem Zielrechner bleiben?

Dies ist zwar grundsätzlich möglich, jedoch nicht empfehlenswert. Ausnahme: Der Controller wird auf den Status **Suspendieren** gesetzt, oder Sie legen einen anderen Wert als den Standardwert für die Richtlinienmethode **rc_def_inactivity** fest. (Ausführliche Informationen finden Sie unter „Tivoli Remote Control-Richtlinienmethoden" auf Seite 74.) Ansonsten sendet der Zielrechner fortlaufend einen Nachrichtenstrom zum Controller. Dadurch wird verhindert, dass andere Administratoren eine Sitzung mit demselben Zielrechner starten können.

Warum sind einige Auswahlmöglichkeiten im Tivoli Remote Control-Dialog abgeblendet?

Der leitende Administrator hat die Richtlinienmethoden so festgelegt, dass die ausgewählten Werte für diesen Parameter nicht geändert werden können.

Welche Zeitlimiteinstellung sollte für Endpunkte gewählt werden?

Die Zeitlimiteinstellung hängt von der jeweiligen Netzwerkkonfiguration ab und davon, welche Produkte vom Tivoli-Managementagenten unterstützt werden. Jede Tivoli Remote Control-Operation benötigt einige Sekunden, weshalb auf einer zuverlässigen Ethernetverbindung ein Zeitlimit von 10 Sekunden ausreichen dürfte. Wenn die Netzwerkverbindung jedoch unzuverlässig oder langsam ist, oder falls andere Produkte neben Tivoli Remote Control den Tivoli-Managementagenten verwenden, kann ein längeres Zeitlimit nötig werden (eventuell bis zu 30 Sekunden). Hierbei ist zu beachten, dass bei Versuchen, eine Verbindung zum Tivoli-Managementagenten herzustellen, die angegebene Zeit zuerst ablaufen muss, bevor sie fehlschlagen, und dass deshalb ein Host ohne Tivoli-Managementagent signifikante Verzögerungen hervorruft, wenn das Zeitlimit zu hoch ist.

Gibt es Fälle, in denen ein Zielrechner nicht gesteuert werden kann (außer, wenn der Zielrechner abgeschaltet ist)?

Sie können den Zielrechner nicht steuern, wenn ein anderer Benutzer dieselbe Maschine steuert oder wenn der Tivoli-Managementagent nicht gestartet oder angemeldet ist.

Wie lässt sich das Tivoli Remote Control-Gateway schließen?

Das Tivoli Remote Control-Gateway ist ein Hintergrundprozess, der auf dem verwalteten Knoten ausgeführt wird, auf dem der Remote Control-Server installiert wurde. Er wird gestartet, sobald eine Tivoli Remote Control-Sitzung beginnt, die ein Gateway benötigt.

Um das Gateway zu schließen, muss der zugehörige Prozess namens **pcgateway** beendet werden.

Das Gateway wird immer beim Schließen von Tivoli Framework geschlossen.

Kann eine Wheel Mouse (z. B. IntelliMouse) auf einem Windows NT-, Windows 2000-, Windows XP oder Windows 98 Second Edition-Zielrechner installiert werden?

Ja, allerdings können während einer aktiven Remote Control-Sitzung nur einfache Mausereignisse fern zugeordnet werden. Wenn auf dem Controller ein ähnliches Gerät verwendet wird, werden Sie nicht in der Lage sein, die Funktionen der Wheel Mouse fern auszuführen.

Was bedeuten die Operationen 'start_target' und 'start_controller'?

Für die Steuerungs- und Überwachungsoperationen wird zuerst der Zielrechnerprozess gestartet und danach der Controller, so dass er eine Verbindung mit dem Zielrechner herstellen kann, um einen Fernzugriff zu ermöglichen. Falls der Zielrechnerprozess nicht gestartet wird, wird der Controller nicht ausgeführt. Die Operationen **start_target** und **start_controller** sind die Methoden, mit denen in Tivoli die Zielrechnerprozesse und Controllerprozesse gestartet werden.

Häufig gestellte Fragen

Bei dem Versuch, eine Remote Control-Sitzung auf einem Endpunkt zu starten, wird die Nachricht angezeigt, dass '.....\pctlcf' nicht gefunden werden kann.

Stellen Sie Folgendes sicher:

- Auf dem Gateway, an dem sich der Endpunkt angemeldet hat, ist die Software für den Remote Control-Server installiert.
- Der Tivoli-Managementagent, der auf der Endpunkt-Workstation ausgeführt wird, gehört zu Tivoli Management Framework Version 3.7.1 oder höher (lcfd Version 91 oder höher).

Wie kann das Verzeichnis geändert werden, in dem die Software für Tivoli Remote Control 3.8-Endpunktcontroller und -zielrechner installiert werden soll?

Der Controller wird im Verzeichnis `lcf\pcremote\<i>\ctl` und der Zielrechner im Verzeichnis `lcf\pcremote\<i>\tgt` installiert. Diese Verzeichnisse können Sie nicht ändern.

Was ist zu tun, wenn eine aktive Remote Control-Sitzung gestartet werden soll, die jedoch den Status 'Suspendieren' hat?

Suchen Sie im Verzeichnis des Zielendpunkts die Datei 'RC_Chat.lck'. Löschen Sie diese Datei.

Befehlszeile

Wenn der Befehl 'wrc' auf einem Linux-Tivoli-Management-Server, Version 4.1, ausgeführt wird, werden entweder Fehlermeldungen angezeigt, die mit Remote Control anscheinend nichts zu tun haben, oder der Befehl 'wrc' bleibt hängen. Wo liegt das Problem?

Möglicherweise ist der Wine-Ressourcencompiler auf Ihrem Linux-Rechner installiert. Führen Sie den Befehl **wrc** aus, um zu ermitteln, ob die Shell die ausführbare Datei **wrc** über das Wine-Entwicklungstoolkit anstatt über die Remote Control-Befehlszeile ausführt.

Um das Problem zu beheben, müssen Sie in der Datei 'setup_env.sh' (oder 'setup_env.csh', wenn Sie die C-Shell ausführen) das Tivoli-Binärverzeichnis vor den Systemverzeichnissen platzieren.

Deinstallation

Was ist zu tun, wenn während der Deinstallation von Tivoli Remote Control auf einem Endpunkt mit Hilfe des Befehls 'wrcuninstep' etwas fehlschlägt?

Überprüfen Sie den Inhalt der Datei 'eqnunist.trc' auf dem Laufwerk, auf dem der Endpunkt installiert ist.

Fehlernachrichten

Bei der Deinstallation eines Remote Control-Proxys unter Linux tritt sinngemäß folgende Fehlernachricht auf:

```
Es wurde keine geeignete JVM gefunden.
Führen Sie das Installationsprogramm erneut mit folgender Option aus:
-is:javahome <JAVA HOME DIR>
```

Um den Remote Control-Proxy zu deinstallieren, müssen Sie 'uninstall.sh' vom Verzeichnis '-uninst' aus ausführen.

Beim Anzeigen eines Tivoli Remote Control-Dialogs tritt sinngemäß folgende Fehlernachricht auf:

```
Vom Dämon 'oserv' wurde ein Fehler
festgestellt:
Angeforderte Ressource nicht gefunden
```

Nach der Installation des Tivoli Remote Control-Servers auf dem Tivoli-Server kann auf jedem verwalteten Knoten in der Tivoli Management Region ein Tivoli Remote Control-Objekt erstellt werden. Damit das Produkt richtig arbeitet, muss sich das Objekt auf einem verwalteten Knoten befinden, auf dem auch die Tivoli Remote Control-Server-Software installiert ist. (Dieses Objekt kann auch auf einer anderen Maschine erstellt worden sein, um das Auflösen von IP-Adressen zu beschleunigen.) Um diesen Fehler zu beseitigen, ist die Tivoli Remote Control-Server-Software auf dem Knoten zu installieren, der den Fehler hervorgerufen hat. Verwenden Sie den Befehl **odstat** auf dem Tivoli-Server, und suchen Sie nach dem Fehler **NOT_FOUND**, um herauszufinden, welcher Knoten die Server-Software benötigt.

Beim Starten von Tivoli Remote Control wird eine Nachricht angezeigt, die besagt, dass der Controller kein Endpunkt sei, obwohl dies der Fall ist. Wo liegt das Problem?

Tivoli Remote Control kann nur von einer Maschine aus verwendet werden, die sich als Endpunkt in der Tivoli Management Region befindet. Das Remote Control-Tool stellt mit Hilfe der Umgebungsvariablen **WD_DISPLAY** fest, welche Maschine das Tool zu öffnen versucht, und sucht den Systemnamen in der Tivoli-Namensregistrierung. Es besteht jedoch auch die Möglichkeit, eine Maschine so zu installieren, dass der Name in der Namensregistrierungsdatenbank nicht mit der Umgebungsvariablen **WD_DISPLAY** übereinstimmt. Dieses Problem lässt sich lösen, indem der Namensregistrierungsdatenbank einfach ein ***Aliasname*** für die Maschine hinzugefügt wird. Wenn beispielsweise der verwaltete Knoten **top_dog** als **Top_dog** installiert ist, kann mit folgendem Befehl ein Aliasname hinzugefügt werden:

```
wregister -r Endpoint top_dog $MNO
```

Dabei gilt: *$MNO* ist die Objekt-ID des Endpunkts.

Mit dem Befehl **wregister** wird der Namensregistrierdatenbank der kleingeschriebene Aliasname des Endpunkts hinzugefügt.

Häufig gestellte Fragen

Anhang C. Bei der Installation geänderte Registrierungsdatenbanken und Dateien

Tivoli Remote Control ändert die Konfigurationsdateien von Maschinen mit Windows 98 Second Edition und OS/2 sowie die Registrierungsdatenbank von Maschinen mit Windows NT, Windows 2000, Windows XP und Windows 98 Second Edition. Diese Änderungen werden in den folgenden Tabellen beschrieben.

Windows Controller-Registrierungsdatenbank

`HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli`

Abschnitt	Installiert	Deinstalliert
Remote Control, Controller	Logging:REG_DWORD:0	
	Trace Length:REG_DWORD:0 (*)	

(*): Nur für Windows 98 Second Edition gültig

Datei von OS/2-Controllern

CONFIG.SYS

Abschnitt	Installiert	Deinstalliert
PATH	*Produkt_Verz;$PATH*	*$PATH*
DPATH	*Produkt_Verz;$DPATH*	*$DPATH*
LIBPATH	*Produkt_Verz;$LIBPATH*	*$LIBPATH*
CALL	*Produkt_Verz*\eqnkctld.exe	
SET RCCTLPATH	*Produkt_Verz*	

Dateien von Windows 98 Second Edition-Zielrechnern

SYSTEM.INI

Abschnitt	Installiert	Deinstalliert
386Enh	device=vdcfd95.386	

Registrierungsdatenbank von Windows 98 Second Edition-Zielrechnern

`HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\`

Abschnitt	Installiert	Deinstalliert
Remote Control, Zielrechner	Trace Length:REG_DWORD:0	
	EnableBreakdown=dword:0x1	

Registrierungsdatenbank von Windows NT-, Windows 2000- und Windows XP-Zielrechnern

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\

Abschnitt	Installiert	Deinstalliert
KeyEx2	ErrorControl:REG_DWORD:0x1	
	Group:REG_SZ:Keyboard Class	
	Start:REG_DWORD:0x2	
	Type:REG_DWORD:0x1	
	DisplayName:REG_SZ:Tivoli Remote Control Keyboard Filter	
MouEx2	ErrorControl:REG_DWORD:0	
	Group:REG_SZ:Pointer Class	
	Start:REG_DWORD:0x2	
	Type:REG_DWORD:0x1	
	DisplayName:REG_SZ:Tivoli Remote Control Pointer Filter	
TGrab	ErrorControl:REG_DWORD:0	
	Start:REG_DWORD:0x1	
	Type:REG_DWORD:0x1	
	BusNumber:REG_DWORD:0	
	DisplayName:REG_SZ:"Tivoli Remote Control Text Grabber"	
	InterfaceType:REG_DWORD:0x5	
Eqnmirdd	Start=dword:0x1	
	ErrorControl=dword:0x1	
	Type=dword:0x1	
	Group=Video	
	ImagePath=System32\DRIVERS\ EQNMIRDD.SYS	
	Tag=dword:0x2	
TME10RC	ErrorControl:REG_DWORD:0x1	
	DisplayName:REG_SZ:"Tivoli Remote Control Service"	
	ImagePath=WINNT\rcserv.exe	
	ObjectName:REG_SZ:"LocalSystem"	
	Start:REG_DWORD:0x2	
	Type:REG_DWORD:0x1	

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eqnmirdd

Bei der Installation geänderte Registrierungsdatenbanken und Dateien

Abschnitt	Installiert	Deinstalliert
Device0	Device Description=IBM Tivoli Remote Control Driver	
	InstalledDisplayDrivers=Eqnmirdd	
	MirrorDriver=dword:0x1	
	VgaCompatible=dword:0	
	Attach.ToDesktop=dword:0x1(*)	

(*): Unter Windows NT heißt es nicht 'Attach.ToDesktop', sondern 'Attached.To-Desktop'.

`HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\`

Abschnitt	Installiert	Deinstalliert
Remote Control, Zielmaschine	EnableMD=dword:0x1	
	EnableBreakdown=dword:0x1	
	MDRunning = dword:0x1	

Dateien von OS/2-Zielrechnern

CONFIG.SYS

Abschnitt	Installiert	Deinstalliert
PATH	*Produkt_Verz;$PATH*	*$PATH*
DPATH	*Produkt_Verz;$DPATH*	*$DPATH*
LIBPATH	*Produkt_Verz;$LIBPATH*	*$LIBPATH*
DEVICE	*Produkt_Verz*\eqnvkbd.sys	
DEVICE	*Produkt_Verz*\eqnrcshd.exe	
CALL	*Produkt_Verz*\eqnrcld.exe	
SET RCTGTPATH	*Produkt_Verz*	

SYSTEM.INI

Abschnitt	Installiert	Deinstalliert
boot	os2shield=*Produkt_Verz*\eqnseada.exe	os2shield=winsheld

OS2.INI

Anwendungsname	Schlüsselname	Installiert	Deinstalliert
PM_ED_HOOKS	MODULENAME	EQNPMGRE	
SYS_DLLS	Load	EQNCLHOT	

Bei der Installation geänderte Registrierungsdatenbanken und Dateien

Anhang D. Befehlszeilenschnittstelle

Sie können Tivoli-Befehle von einem verwalteten Knoten aus verwenden. Dies ist dann sinnvoll, wenn kein Zugriff auf eine grafische Benutzeroberfläche besteht, wie beispielsweise bei der Anmeldung über eine Modemverbindung.

Alle Tivoli-Endbenutzerbefehle beginnen mit einem 'w' (z. B. **wrc** und **wrcmdpcr**).

Befehlszeilensyntax

Auf den Handbuchseiten dieses Anhangs werden die folgenden Sonderzeichen verwendet, um die Befehlssyntax zu definieren:

[ ] Zur Kennzeichnung eines optionalen Arguments. Argumente, die nicht in eckigen Klammern stehen, müssen angegeben werden.

... Gibt an, dass mehrere Werte für das vorhergehende Argument angegeben werden können.

| Gibt an, dass es sich um gegenseitig ausschließende Informationen handelt. Es kann entweder das Argument links des Trennzeichens oder das Argument rechts des Trennzeichens verwendet werden. Es können nicht beide Argumente gleichzeitig bei einer Befehlsausführung verwendet werden.

{ } Grenzt eine Gruppe sich gegenseitig ausschließender Argumente ab, von denen ein Argument erforderlich ist. Wenn die Argumente optional sind, stehen sie in eckigen Klammern ([ ]).

rcproxy

Verwenden Sie den Befehl 'rcproxy', um folgende Aktionen auszuführen:

Befehl	Zweck
rcproxy	Remote Control-Proxy starten
rcproxy -stop	Remote Control-Proxy stoppen
rcproxy -list	Verbindungen zwischen zwei Remote Control-Proxys auflisten
rcproxy -kill Sitzungs-ID	Verbindungen zwischen zwei Remote Control-Proxys beenden

SYNTAX

rcproxy

rcproxy -stop

rcproxy -list

rcproxy -kill *Sitzungs-ID*

BESCHREIBUNG

Mit dem Befehl **rcproxy** können Sie die Remote Control-Proxys und ihre Verbindung verwalten.

Dieser Befehl kann nur von dem Verzeichnis aus ausgeführt werden, in dem die Komponente Tivoli Remote Control Proxy installiert ist.

Berechtigung

senior für die Tivoli Management Region.

Argumente

-stop Stoppt den Remote Control-Proxy.

-list Listet die Verbindungen zwischen Remote Control-Proxys auf.

-kill Beendet eine Verbindung zwischen zwei Remote Control-Proxys.

Sitzungs-ID Gibt die Kennung der Verbindung zwischen zwei Remote Control-Proxys an.

BEISPIELE

In den folgenden Beispielen wird dargestellt, wie die Verbindung zwischen zwei Remote Control-Proxys beendet wird:

1. Mit dem folgenden Befehl können Sie die Kennungen von Remote Control-Verbindungen anzeigen:

   ```
   rcproxy -list
   ```

2. Mit dem folgenden Befehl können Sie die angegebene Verbindung zwischen zwei Remote Control-Proxys beenden:

   ```
   rcproxy -kill Sitzungs-ID
   ```

wcreatecontroller

Erstellt eine Instanz des Klassencontrollers für einen angegebenen Hostnamen.

SYNTAX

wcreatecontroller *Hostname Controllerkennung*

BESCHREIBUNG

Mit dem Befehl **wcreatecontroller** können Sie eine Controllerinstanz definieren. Sie können diesen Befehl verwenden, um einen erweiterten Suchlauf von Remote Control zu vermeiden, wenn Sie das Remote Control-Tool von einem verwalteten Knoten aus starten, der gleichzeitig ein Endpunkt ist und dessen Bezeichnung sich vom Hostnamen unterscheidet.

Dieser Befehl kann nur auf einem verwalteten Knoten ausgeführt werden, auf dem die Komponente Tivoli Remote Control Server installiert ist.

Berechtigung

senior für die Tivoli Management Region.

Argumente

Hostname
Gibt den Hostnamen des Controllers an. Enthält der Name Leerzeichen, muss er in Anführungszeichen (“ ”) gesetzt werden.

Controllerkennung
Gibt die Bezeichnung des Controllers an. Enthält der Name Leerzeichen, muss er in Anführungszeichen (“ ”) gesetzt werden.

BEISPIELE

Im folgenden Beispiel wird eine Instanz des Controllers mit dem Hostnamen **enigma2** und der Kennung **admin_ep** erstellt.

```
wcreatecontroller enigma2 admin_ep
```

wcreaterc

Erstellt ein Remote Control-Tool.

SYNTAX

wcreaterc *RemoteControl_Kennung VerwKnoten_Kennung RichtlBereich_Kennung*

BESCHREIBUNG

Mit dem Befehl **wcreaterc** können Sie ein Remote Control-Tool in einem Richtlinienbereich erstellen.

Dieser Befehl kann nur auf einem verwalteten Knoten ausgeführt werden, auf dem die Komponente Tivoli Remote Control Server installiert ist.

Berechtigung

senior für die Tivoli Management Region.

Argumente

RemoteControl_Kennung
Gibt den Namen des Remote Control-Tools an, das erstellt werden soll. Der Name darf folgende Zeichen nicht enthalten:

- Semikolon (;)
- Pipe (|)
- Umgekehrter Apostroph (`)
- Dollarzeichen ($)
- Öffnende runde Klammer (( )
- Öffnende geschweifte Klammer ({)

Enthält der Name Leerzeichen, muss er in Anführungszeichen (“ ”) gesetzt werden.

VerwKnoten_Kennung
Gibt den Namen des verwalteten Knotens an, auf dem sich das Remote Control-Tool befindet. Enthält der Name Leerzeichen, muss er in Anführungszeichen (“ ”) gesetzt werden.

RichtlBereich_Kennung
Gibt den Namen des Richtlinienbereichs an, in den das Remote Control-Tool eingefügt werden soll. Enthält der Name Leerzeichen, muss er in Anführungszeichen (“ ”) gesetzt werden.

BEISPIELE

Im nachfolgenden Beispiel wird ein Remote Control-Tool namens **rc-enigma2-1** auf dem verwalteten Knoten **enigma2** erstellt und in den Richtlinienbereich **south-region** eingefügt.

```
wcreaterc rc-enigma2-1 enigma2 south-region
```

wdeletecontroller

Löscht eine Instanz des Klassencontrollers für einen angegebenen Hostnamen.

SYNTAX

wdeletecontroller *Hostname*

BESCHREIBUNG

Mit dem Befehl **wdeletecontroller** können Sie eine Instanz des Klassencontrollers löschen.

Dieser Befehl kann nur auf einem verwalteten Knoten ausgeführt werden, auf dem die Komponente Tivoli Remote Control Server installiert ist.

Berechtigung

senior für die Tivoli Management Region.

Argumente

Hostname

Gibt den Hostnamen des Controllers an. Enthält der Name Leerzeichen, muss er in Anführungszeichen (“ ”) gesetzt werden.

BEISPIELE

Im folgenden Beispiel wird die Instanz des Controllers mit dem Hostnamen **enigma2** gelöscht.

```
wdeletecontroller enigma2
```

wrc

Aktiviert eine der Aktionen in Tivoli Remote Control.

SYNTAX

wrc *RemoteControlName Aktion RCZiel [RCController*] [*Optionen*]

BESCHREIBUNG

Mit dem Befehl **wrc** können Sie eine der folgenden Aktionen in Tivoli Remote Control aktivieren:

- Remote Control
- Dateiübertragung
- Chat
- Neustart

Dieser Befehl kann nur auf einem verwalteten Knoten ausgeführt werden, auf dem die Komponente Tivoli Remote Control Server installiert ist.

Berechtigung

Admin für das Remote Control-Tool.

Auf dem Zielrechner müssen Sie über die erforderliche Berechtigungsklasse verfügen, wie unter „Schritt 3: Tivoli Remote Control-Berechtigungsklassen zuordnen" auf Seite 69 beschrieben.

Argumente

RemoteControlName
Gibt den Namen eines Remote Control-Tools an, unter dem Sie arbeiten werden. Enthält der Name Leerzeichen, muss er in Anführungszeichen (" ") gesetzt werden.

Aktion Gibt die angeforderte Aktion an:

- **rc** für Remote Control
- **filexfer** für Dateiübertragung
- **Chat** für Chat
- **reboot** für Neustart

RCZiel Gibt die Kennung des Zielrechners an. Diese Kennung hat folgende Syntax:

```
@Endpoint:<Endpunktkennung>
```

Dabei gilt:

<Endpunktkennung> ist die Bezeichnung für einen Endpunkt. Enthält der Name Leerzeichen, muss er in Anführungszeichen (" ") gesetzt werden.

RCController
Gibt die Bezeichnung des Controllers an. Diese Kennung hat folgende Syntax:

```
@Endpoint:<Endpunktkennung>
```

Dabei gilt:

<Endpunktkennung> ist die Bezeichnung für einen Endpunkt. Enthält der Name Leerzeichen, muss er in Anführungszeichen (" ") gesetzt werden.

Optionen

Eine beliebige Kombination aus den in der folgenden Tabelle aufgeführten Optionen:

Option	Einstellung	Richtlinienmethode	Aktionen
-B:(Y | N)	Desktop-Optimierung	rc_def_backgrnd	rc
-C:(0 | 4 | 8)	Zahl der Farben begrenzen auf: 0 (unbegrenzt); 4 (auf 16 F. begr.); 8 (auf 256 F. begr.)	rc_def_color	rc
-D:<WTSID>	ID der Sitzung der Terminal Server-Workstation, auf der der Controller gestartet wird.		Alle
-J:(Y | N)	Installation von JRE 1.3		filexfer, chat
-G:(0 | 5 | 10 | 15 | 30 | 60 | 120 | 240 | 480 | 960)	Reaktionszeit	rc_def_grace_time	Alle
-P:(Y | N)	Aktion bei Zeitlimitüberschreitung	rc_def_timeout_op	Alle
-R:(50)	Bildwiederholfrequenz	rc_def_rate	rc
-T:(Y | N)	'Status des Zielrechners ändern' aktivieren	rc_def_alt_t	rc
-Z:(Y | N)	Komprimierung aktivieren	rc_def_comp	rc, filexfer
-I:(0...)	Zeitlimitüberschreitung bei Inaktivität	rc_def_inactivity	rc
-S:(A | M)	Anfangsstatus	rc_def_initstate	rc
-Y:(Y | N)	Optimierung bei langsamer Verbindung	rc_def_optimize	rc

Wenn eine Option fehlt oder ungültig ist, wird der Wert verwendet, der von der entsprechenden Richtlinienmethode zurückgegeben wird. Wenn die Richtlinienmethode einen gesperrten Wert zurückgibt, wird der CLI-Wert (falls vorhanden) ignoriert.

Anmerkung:

1. Die Aktionen **monitor**, **controla** und **controlm** der früheren Versionen von Tivoli Remote Control werden unterstützt und haben folgende Bedeutung: **monitor** = Fernsteuerung mit Anfangsstatus 'Überwachen' (wrc rc ... -S:M) **controlm** = Fernsteuerung mit Anfangsstatus 'Überwachen' (wrc rc ... -S:M) **controla** = Fernsteuerung mit Anfangsstatus 'Aktivieren' (wrc rc ... -S:A)

2. Die Option **Auf 16 Farben begrenzen** (-C:(Y|N)) der früheren Versionen von Tivoli Remote Control wird wie folgt interpretiert:
   - **-C:Y = -C:4**
   - **-C:N = -C:0**

BEISPIELE

In den in diesem Abschnitt angegebenen Beispielen wird das Remote Control-Tool **rc-sunnew3-1**, der Zielrechner **enigma2-7003** und der Controller **ap** verwendet.

1. Mit dem nachfolgenden Befehl aktivieren Sie eine Remote Control-Sitzung zwischen dem Zielrechner **enigma2-7003** und dem Controller **ap**.

   ```
   wrc
   rc-sunnew3-1 rc @Endpoint:enigma2-7003
   @Endpoint:ap -B:Y -Z:Y -C:8 -G:15 -P:Y -T:Y
   ```

   Die angeforderten Optionen lauteten:
   - Desktop-Optimierung (-B:Y)
   - 'Komprimierung' aktivieren (-Z:Y)
   - Farben auf Zielrechner auf 256 Farben reduzieren (-C:8)
   - Reaktionszeit = 15 Sekunden (-G:15)
   - Aktion bei Zeitlimitüberschreitung = YES (-P:Y)
   - 'Status des Zielrechners ändern' aktivieren (-T:Y)
2. Mit dem nachfolgenden Befehl aktivieren Sie eine Dateiübertragungssitzung zwischen dem Zielrechner **enigma2-7003** und dem Controller **ap**.

   ```
   wrc rc-sunnew3-1 filexfer @Endpoint: enigma2-7003
   @Endpoint:ap -Z:Y -G:15 -P:Y
   ```

   Die angeforderten Optionen lauteten:
   - 'Komprimierung' aktivieren (-Z:Y)
   - Reaktionszeit = 15 Sekunden (-G:15)
   - Aktion bei Zeitlimitüberschreitung = YES (-P:Y)
3. Mit dem nachfolgenden Befehl aktivieren Sie eine Chat-Sitzung zwischen dem Zielrechner **enigma2-7003** und dem Controller **ap**.

   ```
   wrc rc-sunnew3-1 chat @Endpoint:enigma2-7003
   @Endpoint:ap -G:15 -P:N
   ```

   Die angeforderten Optionen lauteten:
   - Reaktionszeit = 15 Sekunden (-G:15)
   - Aktion bei Zeitlimitüberschreitung = NO (-P:N)
4. Mit dem nachfolgenden Befehl starten Sie den Zielrechner **enigma2-7003** neu.

   ```
   wrc rc-sunnew3-1 reboot @Endpoint:enigma2-7003 -G:15 -P:N
   ```

   Die angeforderten Optionen lauteten:
   - Reaktionszeit = 15 Sekunden (-G:15)
   - Aktion bei Zeitlimitüberschreitung = NO (-P:N)

wrcinstep

Installiert die Tivoli Remote Control-Software auf einem oder mehreren Endpunkten.

SYNTAX

wrcinstep {**-c** | **-t**}*Aktionswerte* {**-l** *Endpunktkennung* | **-f***vollst_qual_Dateiname*} [**-b**]

BESCHREIBUNG

Mit dem Befehl **wrcinstep** wird die Tivoli Remote Control-Software auf einem oder mehreren Endpunkten installiert. Dieser Befehl kann nur auf einem verwalteten Knoten ausgeführt werden, auf dem die Komponente Tivoli Remote Control Server installiert ist.

Berechtigung

- **install_product** oder **super** für die Tivoli Management Region zur Installation von Tivoli Remote Control auf einem oder mehreren Endpunkten.
- **remote_reboot** für die Tivoli Management Region zum Neustart eines oder mehrerer Endpunkte.

Argumente

-c
Installiert die Tivoli Remote Control-Software für Controller-Workstations.

-t
Installiert die Tivoli Remote Control-Software für Zielrechner-Workstations.

Aktionswerte
Gibt die Art der zu installierenden Software an. Gültige Werte sind alle Folgen (ohne Leerzeichen) aus einem oder mehreren der folgenden Token:

- **r** (Remote Control)
- **f** (Dateiübertragung)
- **c** (Chat)
- **b** (Neustart) (Dieses Token wird bei der Installation der Software auf Controller-Workstations ignoriert.)
- **j** (Java Run-time Environment 1.3)(Diese Software wird auf dem Zielrechner und dem Controller installiert. Sie wird installiert, wenn Sie zum ersten Mal eine Dateiübertragungs- oder Chat-Sitzung starten.)
- **l** (Nach der Installation der übersetzten Version von Remote Control auf dem Server wird diese Version auf die Endpunkte heruntergeladen.)

-l *Endpunktkennung*
Gibt den Namen des Endpunkts an.

-f *vollst_qual_Dateiname*
Gibt den vollständig qualifizierten Namen einer Datei mit einer Folge aus Kennungen von Endpunkten an (eine pro Zeile), auf denen die Software installiert werden soll.

-b Startet den Tivoli Remote Control-Zielrechner neu. Diese Option funktioniert nur, wenn ein Neustart zum Bereinigen der Umgebung erforderlich ist. Sie wird nicht unterstützt, wenn der Endpunkt unter OS/2 läuft.

BEISPIELE

Im nachfolgenden Beispiel werden die Controllerkomponenten 'Dateiübertragung' und 'Chat' auf dem Endpunkt **ap** installiert.

```
wrcinstep -c fc -l ap
```

wrcmdpcr

Führt auf einem Zielrechner einen Befehl über eine Eingabeaufforderung aus.

Anmerkungen:

1. Der Befehl **wrcmdpcr** kann nicht in Verbindung mit Befehlen verwendet werden, die eine Benutzereingabe erfordern (z. B. **dir /p**).
2. Wenn Sie den Befehl **wrcmdpcr** unter UNIX oder Windows 2000 über die Bash-Shell ausführen, verwenden Sie \\ anstelle von \ bei der Angaben von Pfaden.

SYNTAX

wrcmdpcr *RemoteControlName RCZiel Befehl* [*Argument* ...]

BESCHREIBUNG

Der Befehl **wrcmdpcr** ist ein Tool zur Fehlerbehebung, das das Beheben von Problemen auf Tivoli Remote Control-Zielrechnern erleichtert. Dieser Befehl kann nur über die Eingabeaufforderung auf einem verwalteten Knoten ausgeführt werden, auf dem die Tivoli Remote Control-Serverkomponente installiert ist.

Berechtigung

remote_probe oder **super** auf dem Endpunkt-Zielrechner.

Argumente

RemoteControlName
: Gibt den Namen eines Remote Control-Tools an. Enthält der Name Leerzeichen, muss er in Anführungszeichen (“ ”) gesetzt werden.

RCZiel
: Gibt den Namen eines Endpunkts an. Dieser Rechner muss ein Zielrechner sein. Enthält der Name Leerzeichen, muss er in Anführungszeichen (“ ”) gesetzt werden.

Befehl
: Gibt einen Befehl an, der über die Eingabeaufforderung ausgeführt wird.

Argument
: Fügt dem Befehl Argumente hinzu. Es können bis zu 4 Argumente angegeben werden.

BEISPIELE

In den in diesem Abschnitt angegebenen Beispielen wird das Remote Control-Tool **RC** und der Endpunkt **rbuyse** verwendet.

1. Mit dem folgenden Befehl können die Umgebungsvariablen auf dem Endpunkt angezeigt werden.

   ```
   wrcmdpcr RC rbuyse set
   ```

   Für einen Endpunkt unter Windows NT wird eine ähnliche Ausgabe wie folgende angezeigt:

   ```
   COMPUTERNAME=GCATASTA
   ComSpec=D:\WINNT35\system32\cmd.exe
   OS=Windows_NT
   Os2LibPath=D:\WINNT35\system32\os2\dll;
   Path=D:\WINNT35\system32;D:\WINNT35;N:\gk\bin;
     d:\msdev\bin;N:\CVS
   PROCESSOR_ARCHITECTURE=x86
   PROCESSOR_IDENTIFIER=x86 Family 5 Model 2 Stepping 5,
     GenuineIntel
   PROCESSOR_LEVEL=5
   PROCESSOR_REVISION=0205
   ```

```
PROMPT=$P$G
SystemRoot=D:\WINNT35
SystemDrive=D:
windir=D:\WINNT35
```

2. Mit folgendem Befehl lässt sich der Inhalt des Verzeichnisses **windows** anzeigen:

   ```
   wrcmdpcr RC rbuyse dir \windows
   ```

   Das Argument **\windows** ist nur dann gültig, wenn der Befehl über eine DOS-Eingabeaufforderung ausgeführt wird. Wird der Befehl von einer UNIX-Maschine aus ausgegeben, muss das Argument in **\\windows** geändert werden.

wrcuninstep

Deinstalliert die Tivoli Remote Control-Software auf einem oder mehreren Endpunkten.

SYNTAX

wrcuninstep {**-c** | **-t**} {**-l** *Endpunktkennung* | **-f** *vollst_qual_Dateiname*} [**-b**]

BESCHREIBUNG

Mit dem Befehl **wrcuninstep** wird die Tivoli Remote Control-Software auf einem oder mehreren Endpunkten deinstalliert. Dieser Befehl kann nur auf einem verwalteten Knoten ausgeführt werden, auf dem die Komponente Tivoli Remote Control Server installiert ist. Am Ende des Deinstallationsprozesses wird die Protokolldatei 'eqnunist.trc' auf dem Laufwerk erstellt, auf dem sich der Endpunkt befindet.

Berechtigung

- **install_product** oder **super** für die Tivoli Management Region zur Deinstallation von Tivoli Remote Control auf einem oder mehreren Endpunkten.
- **remote_reboot** für die Tivoli Management Region zum Neustart eines oder mehrerer Endpunkte.

Argumente

-c	Deinstalliert die Remote Control-Software für Controller-Workstations.
-t	Deinstalliert die Remote Control-Software für Zielrechner-Workstations.
-l *Endpunktkennung*	Gibt die Kennung des Endpunkts an.
-f *vollst_qual_Dateiname*	Gibt den vollständig qualifizierten Namen einer Datei mit einer Folge aus Kennungen von Endpunkten an (eine pro Zeile), auf denen die Software deinstalliert werden soll.
-b	Startet den Tivoli Remote Control-Zielrechner neu. Diese Option funktioniert nur, wenn ein Neustart zum Bereinigen der Umgebung erforderlich ist. Sie wird nicht unterstützt, wenn der Endpunkt unter OS/2 läuft.

BEISPIELE

Im folgenden Beispiel wird der Controller auf dem Endpunkt **ap** deinstalliert.

```
wrcuninstep -c -l ap
```

wrcuninstep

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Dienstleistungen oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Dienstleistungen sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur diese Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremddienstleistungen liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten. Anfragen an obige Adresse müssen auf Englisch formuliert werden.

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogrammes illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

Wird dieses Buch als Softcopy (Book) angezeigt, erscheinen keine Fotografien oder Farbabbildungen.

Marken

IBM, das IBM Logo, Tivoli, AIX, OS/2, Tivoli Enterprise, Tivoli Enterprise Console, pSeries, PowerPC und S/390 sind in gewissen Ländern Marken oder eingetragene Marken der International Business Machines Corporation.

Pentium ist in gewissen Ländern eine Marke der Intel Corporation.

Microsoft, Windows und Windows NT sind in gewissen Ländern Marken der Microsoft Corporation.

UNIX ist in gewissen Ländern eine eingetragene Marke von The Open Group.

Java sowie alle auf Java basierenden Marken und Logos sind in gewissen Ländern Marken bzw. eingetragene Marken der Sun Microsystems, Inc.

Namen anderer Unternehmen, Produkte oder Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.

Glossar

A

Administrator. Siehe Tivoli-Administrator.

B

Benutzer. Eine Person, die die Tivoli-Management-Software verwendet und der mindestens eine Berechtigungsklasse zugeordnet ist.

Berechtigungsklasse. In einer Tivoli-Umgebung eine Berechtigungsklasse, die Tivoli-Administratoren zugewiesen wird und ihnen ermöglicht, die ihnen zugeteilten System-/Netzwerkmanagementaufgaben durchzuführen. Eine Berechtigungsklasse kann für die gesamte Tivoli Management Region oder für eine bestimmte Gruppe von Ressourcen, wie z. B. für die in einem Richtlinienbereich enthaltenen Ressourcen, erteilt werden. Beispiele für Berechtigungsklassen sind: super, senior, admin und user.

Bereich. Siehe Tivoli Management Region.

C

Chat. In Tivoli Remote Control eine Funktion, mit der Tivoli-Administratoren schriftliche Dialoge mit Benutzern von fernen Zielrechnern austauschen können.

Client. In einem Client/Serversystem ein Computersystem oder -prozess, das oder der den Service eines anderen Computersystems oder -prozesses (in der Regel Server genannt) anfordert. Mehrere Clients können gemeinsam auf einen allgemeinen Server zugreifen.

Client/Server. In der Datenfernverarbeitung das Interaktionsmodell in der verteilten Datenverarbeitung, in der ein Programm an einem Standort eine Anforderung an ein Programm an einem anderen Standort sendet und auf die Antwort wartet. Das anfordernde Programm wird Client, das antwortende Programm Server genannt.

Clientdämon. Ein AIX-Prozess, der die Operationen des Clients ausführt.

Controller. In Tivoli Remote Control die vom Administrator verwendete Software zur Ausführung der Funktionen Remote Control (Fernsteuerung), Dateiübertragung oder Chat.

Controller-Proxy. Der Remote Control-Proxy, der anstelle des Controllers eine Verbindung zum Zielrechner herstellt. Siehe auch Zielproxy.

D

Dateiübertragung. In Tivoli Remote Control eine Funktion, mit der Tivoli-Administratoren Dateien oder Verzeichnisse zwischen Controller und Zielrechner übertragen können.

Dämon. Ein Programm, das einen Standardservice im nichtüberwachten Modus ausführt. Einige Dämonen werden automatisch ausgelöst, andere führen ihre Tasks regelmäßig aus.

E

Endpunkt. In einer Tivoli-Umgebung der Agent, der den endgültigen Empfänger für eine beliebige Art von Tivoli-Operation darstellt. Siehe Tivoli-Managementagent.

Endpunktmanager. In einer Tivoli-Umgebung ein Service, der auf dem TMR-Server ausgeführt wird, Gateways Endpunkte zuordnet und die Liste mit den Endpunkten verwaltet.

Endpunktmethode. In einer Tivoli-Umgebung eine Methode, die als Ergebnis einer Anforderung von anderen verwalteten Ressourcen in der Tivoli Management Region auf einem Endpunktclient ausgeführt wird. Die Ergebnisse der Methode werden zunächst an das Gateway und anschließend an die anfordernde verwaltete Ressource weitergeleitet.

F

Ferne Verteilung. In einer Tivoli-Umgebung eine Verteilung an Zielrechner, die sich in einer verbundenen Tivoli Management Region befinden.

G

Gateway. Software, die Services zwischen den Endpunkten und der restlichen Tivoli-Umgebung zur Verfügung stellt.

I

Installationsrepository (IR). In Tivoli Software Installation Service das Verzeichnis mit wieder verwendbaren Installationsimages und anderen von Tivoli Software Installation Service verwendeten Daten.

Internet Protocol (IP) . In der Internet-Protokollgruppe ein verbindungsloses Protokoll, das Daten über ein Netzwerk oder miteinander verbundene Netzwerke

leitet und als Verbindung zwischen den höheren Protokollebenen und dem physischen Netzwerk agiert.

Internetwork Packet Exchange (IPX). Das Netzwerkprotokoll zur Verbindung von Novell-Servern oder Workstations bzw. Routern, die IPX implementieren, mit anderen Workstations. Obwohl vergleichbar mit dem Internet Protocol (IP), verwendet IPX andere Paketformate und eine andere Terminologie.

IPX. Siehe Internet Packet Exchange.

IPX-Agent. Ein PC-Agent, der auf IPX/SPX ausgeführt wird. Hierbei kann es sich nur um den Client eines verwalteten NetWare-Standorts handeln.

O

Object Request Broker (ORB). In der objektorientierten Programmierung eine Software, die als Verbindung dient und den transparenten Austausch von Anfragen und Antworten zwischen Objekten ermöglicht.

oserv. Der Tivoli-Service, der als Object Request Broker (ORB) verwendet wird. Dieser Service wird auf dem TMR-Server und allen verwalteten Knoten ausgeführt. Gegensatz zu 'lcfd'.

P

PC-Agent. In einer Tivoli-Umgebung die auf einem Client-PC installierte Software, die die Ausführung von Tivoli-Operationen auf dem PC ermöglicht. Siehe 'Verwalteter PC-Knoten'.

R

Remote Control (Fernsteuerung). In Tivoli Remote Control eine Funktion, mit der der Tivoli-Administrator eine ferne Zielworkstation steuern kann, die an ein Netzwerk angeschlossen ist.

Remote Control-Proxy. Eine Komponente, mit deren Hilfe viele Rechner auf der einen Seite einer Firewall über einen gemeinsamen Port mit vielen Rechnern auf der anderen Seite der Firewall kommunizieren können.

Remote Control-Tool. In IBM Tivoli Remote Control das Tool, das ferne Operationen ermöglicht, beispielsweise die Fernsteuerung oder den Neustart einer fernen Workstation, die Übertragung von Dateien und das Chatten. Dieses Tool ist als verwaltete Remote Control-Ressource definiert und ist einem Richtlinienbereich zugeordnet.

Ressource. Eine Hardware-, Software- oder Dateneinheit, die durch Tivoli-Management-Software verwaltet wird.

Ressourcenberechtigung. Die Berechtigung, die ein Administrator für bestimmte Ressourcen in der lokalen Tivoli Management Region oder in jeder verbundenen Tivoli Management Region hat (z. B. Richtlinienbereiche oder die Administratorobjektgruppe).

Richtlinie. In einer Tivoli-Umgebung eine Reihe von Regeln, die auf verwaltete Ressourcen angewendet werden. Eine spezielle Regel in einer Richtlinie wird als "Richtlinienmethode" bezeichnet.

Richtlinienbereich. In einer Tivoli-Umgebung eine Gruppe von verwalteten Ressourcen, die mindestens eine allgemeine Richtlinie gemeinsam nutzen und die die Management- oder Organisationsstruktur einer Network-Computing-Umgebung bilden. Administratoren können mit Hilfe von Richtlinienbereichen ähnliche Ressourcen zu Gruppen zusammenfassen, den Zugriff auf Ressourcen definieren, Ressourcen steuern sowie Regeln zur Verwaltung der Ressourcen zuordnen.

Richtliniensatz. Ein Richtlinienobjekt, das eine Gruppe von Managementklassen enthält, die für eine Richtliniendomäne vorhanden sind. In einer Richtliniendomäne können mehrere Richtliniensätze vorhanden sein, es kann jedoch jeweils nur ein Richtliniensatz aktiv sein.

Richtlinienunterbereich. In einer Tivoli-Umgebung ein Richtlinienbereich, der in einem anderen Richtlinienbereich erstellt wurde oder sich in einem anderen Richtlinienbereich befindet. Wenn ein Richtlinienunterbereich erstellt wird, verwendet er anfangs die Ressourcen- und Richtlinienmerkmale des übergeordneten Richtlinienbereichs. Der Tivoli-Administrator kann diese Merkmale dann später ändern, um die Unterschiede zwischen Richtlinienbereich und Unterbereich zu verdeutlichen, bzw. an die besonderen Anforderungen des Unterbereichs anpassen.

S

Sequenced Packet Exchange (SPX). Ein sitzungsorientiertes Netzwerkprotokoll in einer Novell-Umgebung. Es baut auf dem Internet Packet Exchange-Protokoll (IPX) auf, ermöglicht die Flusssteuerung und Fehlerbehebung und gewährleistet die Zuverlässigkeit des physisches Netzwerks.

Server. Eine Funktionseinheit, die Services für einen oder mehrere Clients über ein Netzwerk zur Verfügung stellt, z. B. ein Dateiserver, ein Druckserver oder ein Mail-Server.

SPX. Siehe Sequenced Packet Exchange.

Standardrichtlinie. In einer Tivoli-Umgebung eine Reihe von Ressourcenmerkmalswerten, die einer Ressource bei ihrer Erstellung zugeordnet werden.

T

TCP/IP. Siehe *Transmission Control Protocol/Internet Protocol*.

Tivoli Management Region (TMR). In einer Tivoli-Umgebung ein Tivoli-Server und die ihm zugeordneten Clients. Eine Organisation kann mehrere Bereiche (Tivoli Management Regions) besitzen. Eine Tivoli Management Region bezieht sich auf die physische Konnektivität von Ressourcen, während sich ein Richtlinienbereich auf die logische Organisation von Ressourcen bezieht.

Tivoli NetWare Repeater. In einer Tivoli-Umgebung eine Serveranwendung, die auf einem Novell NetWare-Server installiert ist und eine Liste der verfügbaren Clients für den Server verwaltet. Der Tivoli NetWare Repeater führt zusammen mit dem verwalteten NetWare-Standort die Profilverteilung aus.

Tivoli Remote Control-Gateway. Eine optionale Funktion des Tivoli Remote Control-Servers zur Verarbeitung von Übertragungen zwischen Controllern und Zielrechnern.

Tivoli Software Installation Service. Die Tivoli-Komponente, die eine benutzerfreundliche und effiziente Schnittstelle für die Installation von Tivoli Enterprise-Software zur Verfügung stellt. Software Installation Service verwendet die Tivoli-Multiplexverteilungstechnik und bietet eine automatische Überprüfung der Softwarevoraussetzungen, ein wieder verwendbares Repository mit Installationsimages sowie grafische Schnittstellen und Befehlszeilenschnittstellen für die Implementierung von Tivoli-Produkten auf einer großen Anzahl von Computern.

Tivoli Software Installation Service-Depot. In Tivoli Software Installation Service die Komponente, die Installationsimages (auch für Programmkorrekturen) enthält und die Installation dieser Images auf verteilten Systemen verwaltet. Tivoli-Administratoren greifen über den Tivoli Software Installation Service-Client auf das Depot zu.

Tivoli-Administrator. In einer Tivoli-Umgebung ein Systemadministrator, der zur Ausführung von System-/Netzwerkmanagementaufgaben und zur Verwaltung von Richtlinienbereichen in einem oder mehreren Netzwerken berechtigt ist.

Tivoli-Client. Ein Client eines Tivoli-Servers. Siehe TMR-Client und TMR-Server.

Tivoli-Desktop. In der Tivoli-Umgebung der Desktop, mit dem Systemadministratoren ihre Network-Computing-Umgebungen verwalten.

Tivoli-Installationsimage. In einer Tivoli-Umgebung eine Datei auf einer CD oder in einem Dateisystem, die ein zu installierendes Tivoli-Produkt enthält. Mit einem Tivoli-Installationsimage können Sie Tivoli Management Framework oder eine Anwendung in der Framework-Umgebung installieren. Eine einzelne CD enthält in der Regel ein Tivoli-Installationsimage und ein Tivoli-Upgrade-Image, und eventuell noch mögliche Tivoli-Installationsimages für mehrere Anwendungen.

Tivoli-Management-Gateway. In einer Tivoli-Umgebung ein System zur bidirektionalen Kommunikation mit Tivoli-Managementagenten.

Tivoli-Management-Software. Tivoli Enterprise-Software, mit der Unternehmen ihre Datenverarbeitungsressourcen schnell und mühelos zentral verwalten können (einschließlich kritischer Anwendungen für Unternehmensleistung und Gewinne).

Tivoli-Managementagent. In einer Tivoli-Umgebung ein Agent, der sichere Verwaltungsoperationen ausführt.

Tivoli-Server. Siehe TMR-Server.

Tivoli-Umgebung. Die auf Tivoli Management Framework basierenden Tivoli-Anwendungen, die bei einem bestimmten Kunden installiert sind und der Verwaltung des plattformübergreifenden Netzwerkbetriebs dienen.

Tivoli-Upgrade-Image. In einer Tivoli-Umgebung eine Datei auf einer CD oder in einem Dateisystem mit Aktualisierungen eines Tivoli-Produkts. Ein Tivoli-Upgrade-Image enthält nur die Dateien, die seit der letzten Produktversion geändert wurden, mit Scripts und Befehlen, die zur Installation der neuen Dateien und zur Konfiguration der Datenbank benötigt werden.

TMR-Berechtigungsklasse. In einer Tivoli-Umgebung die Berechtigungsklasse eines Administrators für die lokale Tivoli Management Region (den lokalen Bereich) und jeden verbundenen Bereich. Sie verbreitet die zugeordnete Berechtigungsebene auf alle Ressourcen in diesem Bereich. Wenn ein Tivoli-Administrator z. B. die Berechtigung 'senior' für einen Bereich besitzt, gilt diese Berechtigung auch für jede Ressource in diesem Bereich.

TMR-Client. In einer Tivoli-Umgebung jeder Computer (mit Ausnahme des TMR-Servers), auf dem Tivoli Management Framework installiert ist. Der Dämon 'oserv' wird auf dem TMR-Client ausgeführt, und der TMR-Client verwaltet eine lokale Objektdatenbank. Siehe Tivoli-Client und Tivoli-Server.

TMR-Server. Der Server für eine bestimmte Tivoli Management Region, auf dem das gesamte Tivoli-Softwarepaket gespeichert ist bzw. der auf dieses verweist, einschließlich der vollständigen Objektdatenbank.

U

Untergeordneter Remote Control-Proxy. Der Remote Control-Proxy, der auf dem Rechner ausgeführt wird,

auf dem auch der Gateway-Proxy ausgeführt wird. Siehe auch Übergeordneter Remote Control-Proxy.

Übergeordneter Remote Control-Proxy. Der Remote Control-Proxy, der auf dem Rechner ausgeführt wird, auf dem auch der Endpunktproxy ausgeführt wird. Siehe auch Untergeordneter Remote Control-Proxy.

V

Verwalteter Knoten. In einer Tivoli-Umgebung ein Computersystem, auf dem Tivoli Management Framework installiert ist. Gegensatz zu Endpunkt.

Verwalteter NetWare-Standort. In einer Tivoli-Umgebung eine Ressource, die (a) einen Novell NetWare-Server, auf dem der Tivoli NetWare Repeater installiert ist, und (b) einen oder mehrere Client(s) darstellt. Ein verwalteter NetWare-Standort ermöglicht die Verteilung von Profilen über den NetWare-Server an einen oder mehrere angegebene Client-PCs über TCP/IP oder IPX.

Verwalteter PC-Knoten. In einer Tivoli-Umgebung ein Objekt, das einen Client darstellt. Tivoli Management Framework kann nur mit dem PC-Client kommunizieren, wenn der PC-Agent auf dem PC installiert ist. Client-PCs werden in der Regel als verwaltete PC-Knoten bezeichnet.

Z

Ziel. In Tivoli Remote Control eine ferne Workstation, die von der Controller-Workstation gesteuert wird. Siehe auch Endpunkt.

Zielproxy. Der Remote Control-Proxy, der anstelle des Zielrechners eine Verbindung zum Controller herstellt. Siehe auch Controller-Proxy.

Index

A

Administrator, für Webschnittstelle 65
Agenten 141
Aktion
  Chat 107
  Dateiübertragung 113
  Neustart 106
  Remote Control 101
  starten 93
Aktivieren
  Status 103
  synchronisierte Tastatursitzung 106
Aktivierung der Firewall, Übersicht 4
Alt+Esc 104
Alt+Tab 104
Ändern
  Remote Control-Sitzungsstatus
    über den Controller 102
    über den Zielrechner 103
  RemoteControl_PDO, Standardrichtlinie 71
  Standardeinstellungen des Remote Control-Tools 71
Ändern der Zielmaschinenliste 89
Änderungen in Dateien
  auf einem OS/2-Controller 145
  auf einem OS/2-Zielrechner 147
  auf einem Windows 98-Zielrechner 145
Änderungen in der Registrierungsdatenbank 145, 146
Anpassen
  Richtlinienmethoden 72
  Schnittstelle 87
  Sitzungseinstellungen 90
  Tivoli Remote Control-Webseite 91
  Zielmaschinenliste 87
Anzeigen, Menü 102
Austauschen von Nachrichten 109
Automatische Installation, Remote Control-Proxy 49

B

Beenden
  Chat-Sitzung 107
  Dateiübertragung 113
Beenden, Status 103
Befehle
  odadmin 65
  odstat 143
  rcproxy 150
  wcreatecontroller 151
  wcreaterc 68, 152
  wcrtpol 71
  wep sync_gateways 70
  wgetpolm 72
  widmap 8
  winstall 13
  wmv 70, 140
Befehle *(Forts.)*
  wpatch 21
  wputpolm 72
  wrc 154
  wrcinstep 157
  wrcmdpcr 159
  wrcuninstep 161
  wregister 143
  wstarthttpd 91
  wstophttpd 91
  wuninst 23
Befehlszeilensyntax 149
Berechtigungsklassen
  zuordnen 69
Berechtigungsklassen, Übersicht 2
Betriebssysteme, unterstützte 10

C

Chat
  Dialog 108
  Dialoge protokollieren 110
  erneut aktivieren 109
  Nachrichten austauschen 109
  Protokollieren, Option 110
  Remote Control verwenden 111
  starten 107
  stoppen 107
  suspendieren 109
children-cm-info (Abschnitt), übergeordneter Proxy 54
communication-layer, Abschnitt
  übergeordneter Proxy 51
  untergeordneter Proxy 53
config.sys, Datei 145, 147
Controller
  Änderungen in der Windows-Registrierungsdatenbank 146
  Änderungen in OS/2-Dateien 145
  chatten 109
  Dateiübertragungsinformationen protokollieren 118
  Definition 1
  deinstallieren 22, 23
  Ereignisse protokollieren 130
  installieren 14
  OS/2-Traces festlegen 127
  Protokollieren von Chat-Informationen 119
  Registrierungsdatenbankänderungen unter Windows 145
  Remote Control-Informationen protokollieren 117
  Remote Control-Traces auf Windows-Systemen festlegen 122
  Sitzungsstatus ändern 102
  verwenden 101, 102
  Windows-Traces festlegen 124, 126
createrc, Befehl 152

D

Datei, Menü 102
Dateien
  config.sys 145, 147
  os2.ini 147
  rcproxy.cfg 51, 58
  rcproxy.route 58
  system.ini 145, 147
Dateiübertragung
  Dateien kopieren 115
  Dialog 114
  protokollieren 117
  starten 113
  stoppen 113
  Verzeichnisse erstellen 115
  Verzeichnisse oder Dateien löschen 115
Datenbank, Integration 16
Datenbank für Tivoli Inventory, Integration 16
Datenverschlüsselung 4
default.html, Seite, Anpassung 91
Definieren
  übergeordneter Proxy 31
  untergeordneter Proxy 31
Definition
  Controller-Proxy 25
  Remote Control-Gateway 2
  Remote Control-Proxy 1
  Remote Control-Server 1
  Zielproxy 25
Deinstallieren
  Controller 22, 23
  Gateway 22
  Remote Control-Proxy 23
  Server 22
  Zielrechner 22, 23
Dialoge
  Tivoli Remote Control 102

E

E-Mail-Kontakt x
Editieren
  rcproxy.cfg 51, 58
Einführung 1
Eingabehilfen 137
Eingeschränkter Modus, Sitzung 16
Einstellungen, Remote Control-Tool 71
Endpunkt
  Controller, Installation 14
  Fehler protokollieren 132
  Ziel, Installation 14
Erforderliche Benutzerberechtigungen 8
Erneutes Aktivieren einer Chat-Sitzung 109
Erstellen von Verzeichnissen 115

F

FAQs 139
Fehlerbehebung 117
  Zeitlimiteinstellung 141
Fehlernachrichten
  Host ist kein verwalteter Knoten 143
  Host ist kein verwalteter PC-Knoten 143
  Remote Control-Proxy deinstallieren 143
  Ressource nicht gefunden 143
  start_controller 141
  start_target 141
Ferner Modus 104
Fernverbindungen, Instrumentierung 65
Festlegen
  rc_def_define
    DefinableTargetList 88
    FilteredList 88
    UncheckedList 89
  rc_def_proxy 33
  Traces
    auf einem OS/2-Controller 127
    auf einem OS/2-Zielrechner 127
    auf einem Windows 98-Zielrechner 124
    auf einem Windows-Controller 122, 124, 126
    auf einem Windows-Zielrechner 122, 124, 126
    auf Tivoli Remote Control-Server 121
    auf Tivoli-Server 132
Firewall
  Beispielszenario 59
  Identifikation von Szenarios 25
  Szenarios mit Firewall Security Toolbox 26
  Szenarios mit Proxy im Standalone-Modus 31

G

Gateway
  deinstallieren 22
  installieren 16
  schließen 141
  starten 99
Generierung von Hinweisen 3

H

Handbücher
  Bestellungen ix
  online ix
  Rückmeldung ix
Hardware, Voraussetzungen 7
Häufig gestellte Fragen 139
Hilfe, Menü 102
Hinzufügen
  Controller 151
  Remote Control als verwaltete Ressource 67
  Zielrechner 70

I

Identifikation
  Firewall-Szenarios 25
IME-Sprungtaste 105
Installation planen 5
Installieren 14
  Änderungen in Dateien 145
  auf Endpunkten 14
  Controller 14
  planen 5
  Remote Control-Gateway 16
  Remote Control-Proxy 17
  Remote Control-Proxy im Standalone-Modus 40
  Remote Control-Proxy zusätzlich zu Toolbox-Proxys 34
  Tivoli Remote Control-Gateway 16
  Tivoli Remote Control-Server 12
    mit 'winstall' 13
    mit SIS 12
    über den Tivoli-Desktop 12
  Übersicht 9
  Verzeichnisse 10
  Zielrechner 14
Integration mit der Datenbank für Tivoli Inventory 16

K

Komponenten 10
Konfigurieren
  Pfade für untergeordnete Proxys 58
  Remote Control-Proxy 51
  Richtlinienbereiche 67
Kopieren von Dateien 115
Kundenunterstützung xi

L

Leistung 133
log, Abschnitt
  übergeordneter Proxy 51
  untergeordneter Proxy 51
Lokaler Modus 104
Löschen von Verzeichnissen oder Dateien 115

M

Menüs
  Anzeigen 102
  Datei 102
  Hilfe 102
  Status 102
  Tastenkombinationen 102
Methoden, Übersicht 73
Methoden für die Standardrichtlinie 74
Modi, Tastatur 104

N

Neustart, Aktion 106

O

odadmin, Befehl 65
odstat, Befehl 143
Onlineveröffentlichungen ix
OS/2-Gateway, Einschränkungen bei der Tastatureingabe 105
os2.ini, Datei 147

P

parent-cm-info section (Abschnitt), untergeordneter Proxy 55
pcgateway, Prozess 141
pcremoteaccess.cgi, Script 91
Pfad für untergeordnetes Proxy definieren 58
Pfadnamen, Schreibweise xi
Problembestimmung 117
  Tastaturbelegungsprotokoll 133
  Workstation-Konfigurationsbericht 132
Protokolldateien
  für Chat 119
  für die Installation 121
  für Remote Control 117
  Inhalt 120
  zur Dateiübertragung 118
Protokolle, unterstützte 10
Protokolle und Traces, Übersicht 3
Protokollieren
  Anwendungsereignisse 130
  Chat-Dialoge 110
  Chat-Informationen 119
  Dateiübertragungsinformationen 118
  Endpunktfehler 132
  Installationsinformationen 121
  Remote Control-Informationen 117
Protokollieren von Chat-Ereignissen 110
Proxy
  Befehlszeile 150
  Beispielszenario 59
  deinstallieren 22, 23
  Firewall Security Toolbox 26
  Identifikation von Szenarios 25
  installieren 17
  konfigurieren 51
  Standalone-Modus 31
  starten 99
  übergeordnet 31
  untergeordnet 31

R

rc_def_alt_t, Richtlinienmethode 74
rc_def_backgrnd, Richtlinienmethode 75
rc_def_cmmand, Richtlinienmethode 76
rc_def_color, Richtlinienmethode 75
rc_def_comp, Richtlinienmethode 76
rc_def_define, Richtlinienmethode 77
rc_def_encryption, Richtlinienmethode 77
rc_def_ftmode, Richtlinienmethode 78
rc_def_grace_time, Richtlinienmethode 78
rc_def_gw, Richtlinienmethode 79
rc_def_inactivity, Richtlinienmethode 79
rc_def_initstate, Richtlinienmethode 80

rc_def_optimize, Richtlinienmethode 80
rc_def_polfilter_mode, Richtlinienmethode 80
rc_def_ports, Richtlinienmethode 81
rc_def_proxy, Richtlinienmethode 82
rc_def_rate, Richtlinienmethode 83
rc_def_rcmode, Richtlinienmethode 83
rc_def_targets, Richtlinienmethode 84
rc_def_timeout_op, Richtlinienmethode 84
rc_def_uncheckedlist, Richtlinienmethode 84
RCACTN, Parameter 91
RCCTRL, Parameter 91
rcproxy, Abschnitt
  übergeordneter Proxy 56
  untergeordneter Proxy 56
rcproxy, Befehl 150
rcproxy.cfg
  parent-cm-info, Abschnitt 55
rcproxy.cfg, Datei 51, 58
  children-cm-info 54
  communication-layer, Abschnitt 53
  log, Abschnitt 51
  rcproxy, Abschnitt 56
rcproxy.log, Datei
  communication-layer, Abschnitt 51
rcproxy.route, Datei 58
RCTARG, Parameter 91
RCTOOL, Parameter 91
Remote Control
  Aktion 101
  Sitzung
    starten 101
    stoppen 101
Remote Control, Fenster 102
Remote Control-Controller
  verwenden 102
Remote Control-Proxy
  automatische Installation 49
  Definition 1
  installieren 17
  konfigurieren 51
  starten 99
  übergeordneten Proxy definieren 31
  untergeordnetes Element definieren 31
Remote Control-Server
  deinstallieren 22
  installieren 12
Remote Control-Tool
  Standardeinstellungen 71
Remote Control-Tool erstellen 67
Remote Control-Zielrechner
  verwenden 103
RemoteControl_PDO 72
RemoteControl_PDO, Standardrichtlinie 71
Richtlinienbereich
  konfigurieren 67
  Ziele zuordnen 70
Richtlinienmethoden
  rc_def_alt_t 74
  rc_def_backgrnd 75
  rc_def_color 75
  rc_def_command 76
  rc_def_comp 76
Richtlinienmethoden *(Forts.)*
  rc_def_define 77
  rc_def_encryption 77
  rc_def_ftmode 78
  rc_def_grace_time 78
  rc_def_gw 79
  rc_def_inactivity 79
  rc_def_initstate 80
  rc_def_optimize 80
  rc_def_polfilter_mode 80
  rc_def_ports 81
  rc_def_proxy 82
  rc_def_rate 83
  rc_def_rcmode 83
  rc_def_targets 84
  rc_def_timeout_op 84
  rc_def_uncheckedlist 84
  Übersicht 73
Rückmeldung zu Veröffentlichungen x

S

Sammeln von Informationen
  Tastaturbelegungsprotokoll 132
  Workstation-Konfigurationsbericht 132
Schnittstellenanpassung 87
Schreibweise
  Pfadnamen xi
  Schriftbild xi
  Umgebungsvariablen xi
Script, pcremoteaccess.cgi 91
Senden
  Alt+Esc 104
  Alt+Tab 104
  IME-Sprungtaste 105
  Strg+Alt+Entf 105
  Strg+Esc 104
  Strg+Umschalt+Esc 105
  Systemtastenkombinationen 104
Server
  deinstallieren 22
  installieren 12
Sicherheitsstufen 2
Sitzung
  Einstellungsanpassung
    über die grafische Benutzerschnittstelle 90
    über die Webschnittstelle 90
  Status 102
  über Firewalls 25
Sitzungen über Firewalls ausführen 25
Software, Voraussetzungen 8
Spiegeltreiber unter Windows XP 15
Standardrichtlinie
  Änderungen 71
  Methodenliste 74
Standardrichtlinie, Übersicht 3
Starten
  Aktion 93
    über den Tivoli-Desktop 93
    über die Befehlszeile 98
    über eine Terminal Server-Umgebung 97
    über einen Web-Browser 95
  Chat-Sitzung 107
  Dateiübertragungssitzung 113
  Remote Control-Gateway 99
Starten *(Forts.)*
  Remote Control-Proxy 99
  Remote Control-Sitzung 101
startsession.cgi, Script 91
Status
  Aktivieren 103
  Beenden 103
  Suspendieren, Option 103
  Überwachen 103
Status, Menü 102
Steigern der Leistung 133
Stoppen
  Chat-Sitzung 107
  Dateiübertragungssitzung 113
  Remote Control-Sitzung 101
Strg+Alt+Entf 105
Strg+Esc 104
Strg+Umschalt+Esc 105
Stufen
  Sicherheit 2
Suspendieren, Status 103
Suspendieren einer Chat-Sitzung 109
Synchronisation von Tastaturen 106
system.ini, Datei 145, 147
Systemtastenkombinationen, senden 104
Szenario mit Firewalls 59
Szenarios mit dem Remote Control-Proxy im Standalone-Modus 31
Szenarios mit Firewall Security Toolbox 26
Szenarios mit Remote Control-Proxy im Standalone-Modus 58

T

Tastatur
  gemischte Unterstützung 105
  Modi 104
  Synchronisation 106
Tastatureingabe, Einschränkungen 105
Tastenkombinationen, Menü 102
Tivoli-Desktop
  Fernverbindung, Instrumentierung 65
Tivoli-Kundenunterstützung xi
Tivoli Remote Control
  Berechtigungsklassen 69
  deinstallieren 22
  Protokolle 117
  Webseitenanpassung 91
Tivoli Remote Control, Dialog 102
Tivoli Remote Control-Gateway
  Definition 2
  installieren 16
Tivoli Remote Control-Server
  Definition 1
  Installationsinformationen protokollieren 121
  Traces festlegen 121
Tivoli Remote Control-Traces 121
Tivoli-Server
  Traces festlegen 132
Tivoli-Server, Fernverbindungen 65
Tivoli-Umgebung, Beispiel 2
Tool
  Einstellungen 71
  erstellen 67

Tracedateien
für Remote Control 122, 124
Inhalt 127
unter OS/2 127

U

Übergeordneter Proxy 31
children-cm-info 54
communication-layer 51
log 51
rcproxy 56
Überwachen, Status 103
Umgebungsvariablen, Schreibweise xi
Umschalten in andere Tastaturmodi 104
Untergeordneter Proxy 31
log 51
parent-cm-info 55
Pfad definieren 58
rcproxy 56
Übertragungsebene 53
Unterstützte Betriebssysteme 10
Unterstützte Protokolle 10
Unterstützte Tastaturen 105
Unterstützung für unterschiedliche Tastaturen 105
Upgrade ausführen
einzelner Bereich 17
verbundene Bereiche 22
Upgrade-Methoden 20
Befehl 'wpatch' verwenden 21
SIS verwenden 20
Tivoli-Desktop verwenden 20

V

Variablen
WD_DISPLAY 143
Variablen, Schreibweise xi
Verbindungen, Instrumentierung 65
Veröffentlichungen
Bestellungen ix
online ix
Rückmeldung ix
Veröffentlichungen bestellen x
Verschlüsselung, Übersicht 4
Verwaltete Remote Control-Ressource 67
Verwaltete Ressource, Remote Control 67
Verwenden
Controller 101, 102
Zielrechner 103
Verzeichnisnamen, Schreibweise xi
Vollständig funktionsfähiger Modus
eingeschränkter Modus 16
vollständig funktionsfähiger Modus 16
Vollständig funktionsfähiger Modus, Sitzung 16
Voraussetzungen
Hardware 7
Software 8

W

wcreatecontroller, Befehl 151
wcreaterc, Befehl 68
wcrtpol, Befehl 71
WD_DISPLAY, Variable 143
Webschnittstelle
Fernverbindung, Instrumentierung 65
Webschnittstelle, Administrator definieren 65
Webseite, Anpassung 91
wep sync_gateways, Befehl 70
wgetpolm, Befehl 72
Wheel Mouse 141
widmap, Befehl 8
Windows XP, Spiegeltreiber 15
winstall, Befehl 13
wmv, Befehl 70, 140
wpatch, Befehl 21
wputpolm, Befehl 72
wrc, Befehl 154
wrcinstep, Befehl 157
wrcmdpcr, Befehl 159
wrcuninstep, Befehl 161
wregister, Befehl 143
wstarthttpd, Befehl 91
wstophttpd, Befehl 91
wuninst, Befehl 23

Z

Zeitlimiteinstellung 141
Zielrechner
Änderungen in der Windows 98-Registrierungsdatenbank 145
Änderungen in der Windows-Registrierungsdatenbank 146
Änderungen in OS/2-Dateien 147
Chat-Informationen protokollieren 119
chatten 109
Dateiübertragungsinformationen protokollieren 118
Definition 1
deinstallieren 22, 23
installieren 14
Liste 87
OS/2-Traces festlegen 127
Proxyanpassung 33
Remote Control-Informationen protokollieren 117
Remote Control-Traces auf Windows 98-Systemen festlegen 124
Remote Control-Traces auf Windows-Systemen festlegen 122
Sitzungsstatus ändern 103
Verbindung bestehen lassen 140
verwenden 103
Windows 98-Dateiänderungen 145
Windows-Traces festlegen 124, 126
zu einem Richtlinienbereich zugeordnet 70
Zielrechner schnell laden 135
Zuordnen
neue Standardrichtlinie 73
Zuordnen *(Forts.)*
Tivoli Remote Control-Berechtigungsklassen 69
Ziele zu Richtlinienbereichen 70

SC12-3220-00